

# Red Hat Enterprise Linux 5.5

## Technical Notes

Detailed notes on the changes implemented  
in Red Hat Enterprise Linux 5.5



# Red Hat Enterprise Linux 5.5 Technical Notes

## Detailed notes on the changes implemented in Red Hat Enterprise Linux 5.5

### Edition 0

Author

[rhelv5-list@redhat.com](mailto:rhelv5-list@redhat.com)

Copyright © 2010 Red Hat.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at <http://creativecommons.org/licenses/by-sa/3.0/>. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, MetaMatrix, Fedora, the Infinity Logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux® is the registered trademark of Linus Torvalds in the United States and other countries.

Java® is a registered trademark of Oracle and/or its affiliates.

XFS® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

All other trademarks are the property of their respective owners.

1801 Varsity Drive  
Raleigh, NC 27606-2072 USA  
Phone: +1 919 754 3700  
Phone: 888 733 4281  
Fax: +1 919 754 3701

The Red Hat Enterprise Linux 5.5 Technical Notes list and document the changes made to the Red Hat Enterprise Linux 5 operating system and its accompanying applications between minor release Red Hat Enterprise Linux 5.4 and minor release Red Hat Enterprise Linux 5.5.

<b>1. Package Updates</b>	<b>1</b>
1.1. acl .....	1
1.2. acpid .....	2
1.3. aide .....	3
1.4. anaconda .....	3
1.5. apr-util .....	8
1.6. at .....	8
1.7. audit .....	9
1.8. autofs .....	10
1.9. automake .....	12
1.10. avahi .....	13
1.11. bind .....	13
1.12. binutils .....	15
1.13. bogl .....	16
1.14. bootparamd .....	16
1.15. booty .....	17
1.16. brltty .....	17
1.17. checkpolicy .....	18
1.18. chkconfig .....	19
1.19. cman .....	20
1.20. cmirror .....	25
1.21. cmirror-kmod .....	26
1.22. conga .....	26
1.23. coolkey .....	28
1.24. coreutils .....	29
1.25. cpio .....	30
1.26. cpuspeed .....	30
1.27. crash .....	31
1.28. ctdb .....	32
1.29. cups .....	33
1.30. curl .....	36
1.31. cyrus-imapd .....	37
1.32. cyrus-sasl .....	37
1.33. dbus .....	38
1.34. dbus-python .....	39
1.35. device-mapper .....	39
1.36. device-mapper-multipath .....	40
1.37. dhcp .....	42
1.38. dhcpv6 .....	44
1.39. dmidecode .....	45
1.40. dmraid .....	46
1.41. dogtail .....	47
1.42. dosfstools .....	48
1.43. dstat .....	48
1.44. e4fsprogs .....	49
1.45. elilo .....	49
1.46. elinks .....	50
1.47. esc .....	51
1.48. etherboot .....	52
1.49. ethtool .....	52

1.50. evince .....	53
1.51. exim .....	54
1.52. fetchmail .....	55
1.53. filesystem .....	56
1.54. firefox .....	56
1.55. firstboot .....	60
1.56. freeradius .....	61
1.57. gail .....	62
1.58. gcc .....	62
1.59. gd .....	64
1.60. gdb .....	65
1.61. gfs-kmod .....	66
1.62. gfs-utils .....	67
1.63. gfs2-utils .....	68
1.64. glibc .....	69
1.65. gnome-vfs2 .....	70
1.66. gpart .....	72
1.67. gzip .....	73
1.68. hal .....	73
1.69. hmscalc .....	74
1.70. httpd .....	75
1.71. hwdata .....	77
1.72. ia32el .....	78
1.73. iasl .....	79
1.74. inn .....	80
1.75. iproute .....	80
1.76. iprutils .....	81
1.77. iptables .....	81
1.78. iptstate .....	82
1.79. ipw2200-firmware .....	82
1.80. iscsi-initiator-utils .....	82
1.81. iwl3945-firmware .....	84
1.82. iwl4965-firmware .....	84
1.83. iwl5000-firmware .....	85
1.84. java-1.6.0-ibm .....	85
1.85. java-1.6.0-openjdk .....	86
1.86. java-1.6.0-sun .....	87
1.87. kdelibs .....	88
1.88. kernel .....	89
1.89. kexec-tools .....	128
1.90. krb5 .....	131
1.91. ksh .....	131
1.92. ktune .....	133
1.93. kudzu .....	135
1.94. kvm .....	135
1.95. less .....	143
1.96. libXi .....	144
1.97. libXrandr .....	145
1.98. libXt .....	145
1.99. libaio .....	145
1.100. libcmptutil .....	146

---

1.101. libevent .....	146
1.102. libgnomecups .....	147
1.103. libgtop2 .....	147
1.104. libhugetlbfs .....	148
1.105. libsepol .....	148
1.106. libuser .....	149
1.107. libvirt .....	149
1.108. libvirt-cim .....	154
1.109. libvorbis .....	156
1.110. linuxwacom .....	156
1.111. lm_sensors .....	156
1.112. log4cpp .....	157
1.113. logwatch .....	158
1.114. lvm2 .....	159
1.115. lvm2-cluster .....	161
1.116. man-pages .....	163
1.117. man-pages-ja .....	164
1.118. mcelog .....	166
1.119. mdadm .....	166
1.120. mesa .....	167
1.121. metacity .....	167
1.122. microcode_ctl .....	169
1.123. mkinitrd .....	170
1.124. module-init-tools .....	172
1.125. mtx .....	172
1.126. mysql .....	173
1.127. nautilus-open-terminal .....	175
1.128. neon .....	175
1.129. net-snmp .....	176
1.130. net-tools .....	178
1.131. NetworkManager .....	179
1.132. newt .....	180
1.133. nfs-utils .....	181
1.134. nspluginwrapper .....	182
1.135. nss_ldap .....	182
1.136. numactl .....	184
1.137. openCryptoki .....	185
1.138. openais .....	186
1.139. OpenIPMI .....	188
1.140. openib .....	189
1.141. openldap .....	191
1.142. openmotif .....	192
1.143. openoffice.org .....	193
1.144. openssh .....	195
1.145. openssl .....	197
1.146. openswan .....	198
1.147. oprofile .....	200
1.148. pam .....	201
1.149. pam_krb5 .....	201
1.150. paps .....	202
1.151. parted .....	202

1.152. pax .....	203
1.153. pciutils .....	204
1.154. pcsc-lite .....	204
1.155. perl-Sys-Virt .....	205
1.156. perl-XML-SAX .....	206
1.157. pexpect .....	207
1.158. php .....	207
1.159. pidgin .....	209
1.160. piranha .....	210
1.161. pirut .....	211
1.162. policycoreutils .....	211
1.163. poppler .....	212
1.164. postgresql .....	213
1.165. ppc64-utils .....	214
1.166. procps .....	215
1.167. pykickstart .....	216
1.168. python-virtinst .....	217
1.169. PyXML .....	218
1.170. qspice .....	219
1.171. readahead .....	221
1.172. redhat-artwork .....	222
1.173. redhat-release .....	222
1.174. redhat-release-notes .....	222
1.175. rgmanager .....	223
1.176. rhn-client-tools .....	226
1.177. rhnlib .....	227
1.178. rhnsd .....	228
1.179. rhppl .....	228
1.180. rsyslog .....	229
1.181. ruby .....	230
1.182. samba .....	230
1.183. samba3x .....	233
1.184. sblim .....	234
1.185. screen .....	235
1.186. scsi-target-utils .....	236
1.187. selinux-policy .....	237
1.188. sendmail .....	242
1.189. shadow-utils .....	243
1.190. sosreport .....	244
1.191. squid .....	248
1.192. squirrelmail .....	249
1.193. star .....	250
1.194. strace .....	250
1.195. sudo .....	251
1.196. sysklogd .....	253
1.197. system-config-cluster .....	254
1.198. system-config-lvm .....	255
1.199. system-config-securitylevel .....	256
1.200. system-config-services .....	257
1.201. systemtap .....	258
1.202. tar .....	261

1.203. taskjuggler .....	263
1.204. tcpdump .....	264
1.205. tcsh .....	264
1.206. tog-pegasus .....	266
1.207. util-linux .....	267
1.208. valgrind .....	267
1.209. vconfig .....	268
1.210. vino .....	268
1.211. virt-manager .....	269
1.212. vixie-cron .....	270
1.213. vsftpd .....	271
1.214. wdaemon .....	271
1.215. wget .....	271
1.216. wpa_supplicant .....	272
1.217. xen .....	272
1.218. xerces-j2 .....	277
1.219. xmlsec1 .....	278
1.220. xorg-x11-drivers .....	278
1.221. xorg-x11-drv-ast .....	279
1.222. xorg-x11-drv-evdev .....	279
1.223. xorg-x11-drv-fbdev .....	279
1.224. xorg-x11-drv-i810 .....	280
1.225. xorg-x11-drv-mga .....	280
1.226. xorg-x11-drv-nv .....	281
1.227. xorg-x11-drv-qxl .....	281
1.228. xorg-x11-drv-vesa .....	283
1.229. xorg-x11-server .....	283
1.230. xorg-x11-xdm .....	285
1.231. xterm .....	285
1.232. yaboot .....	286
1.233. yp-tools .....	286
1.234. yum .....	287
1.235. yum-rhn-plugin .....	288
<b>2. New Packages</b> .....	<b>289</b>
2.1. RHEA-2010:0305: freeradius2 .....	289
2.2. RHEA-2010:0240: gpxe .....	289
2.3. RHEA-2010:0199: gsl .....	290
2.4. RHEA-2010:0217: iwl1000-firmware .....	290
2.5. RHEA-2010:0220: iwl6000-firmware .....	290
2.6. RHEA-2010:0276: postgresql84 .....	290
2.7. RHEA-2010:0268: python-dmidecode .....	291
2.8. RHEA-2010:0249: tunctl .....	292
2.9. RHEA-2010:0189: xz .....	292
<b>3. Technology Previews</b> .....	<b>293</b>
<b>4. Capabilities and Limits</b> .....	<b>299</b>
<b>5. Known Issues</b> .....	<b>301</b>
5.1. anaconda .....	301
5.2. cmirror .....	304
5.3. compiz .....	304

5.4. ctdb .....	305
5.5. device-mapper-multipath .....	305
5.6. dmraid .....	306
5.7. dogtail .....	307
5.8. firstboot .....	307
5.9. gfs2-utils .....	308
5.10. gnome-volume-manager .....	308
5.11. initscripts .....	309
5.12. iscsi-initiator-utils .....	309
5.13. kernel-xen .....	309
5.14. kernel .....	312
5.15. kexec-tools .....	317
5.16. krb5 .....	318
5.17. kvm .....	318
5.18. less .....	322
5.19. libcmpiutil .....	322
5.20. libvirt .....	322
5.21. lvm2 .....	322
5.22. mesa .....	323
5.23. mkinitrd .....	323
5.24. openib .....	323
5.25. openmpi .....	324
5.26. qspice .....	324
5.27. systemtap .....	324
5.28. virtio-win .....	325
5.29. xorg-x11-drv-i810 .....	325
5.30. xorg-x11-drv-nv .....	326
5.31. xorg-x11-drv-vesa .....	326
5.32. yaboot .....	327
5.33. xen .....	327
<b>A. Package Manifest</b> .....	<b>329</b>
A.1. Added Packages .....	329
A.2. Dropped Packages .....	331
A.3. Updated Packages .....	331
<b>B. Revision History</b> .....	<b>459</b>



---

# Preface

The Red Hat Enterprise Linux 5.5 Technical Notes list and document the changes made to the Red Hat Enterprise Linux 5 operating system and its accompanying applications between minor release Red Hat Enterprise Linux 5.4 and minor release Red Hat Enterprise Linux 5.5.

For system administrators and others planning Red Hat Enterprise Linux 5.5 upgrades and deployments, the Technical Notes provide a single, organized record of the bugs fixed in, features added to, and Technology Previews included with this new release of Red Hat Enterprise Linux.

For auditors and compliance officers, the Red Hat Enterprise Linux 5.5 Technical Notes provide a single, organized source for change tracking and compliance testing.

For every user, the Red Hat Enterprise Linux 5.5 Technical Notes provide details of what has changed in this new release.

The Technical Notes also include, as an Appendix, the Red Hat Enterprise Linux Package Manifest: a listing of every changed package in this release.



# Package Updates

## 1.1. acl

### 1.1.1. RHBA-2009:1652: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata *RHBA-2009:1652*<sup>1</sup>

Updated acl packages that fix a bug are now available.

Access Control Lists (ACLs) are used to define finer-grained discretionary access rights for files and directories. The acl packages contain the getfacl and setfacl utilities needed for manipulating access control lists.

This update fixes the following bug:

\* the "setfacl" command, which sets the access control lists for files, always returned an exit status of 0, even when the command failed and printed out error messages. With this update, setfacl exits with the correct exit status upon failure. ([BZ#368451](https://bugzilla.redhat.com/show_bug.cgi?id=368451))<sup>2</sup>

\* running "setfacl -- --test" caused setfacl to segmentation fault. This has been fixed in this update. ([BZ#430458](https://bugzilla.redhat.com/show_bug.cgi?id=430458))<sup>3</sup>

\* running the "setfacl" command with the '-P' flag, which is the short form of the '--physical' option, which is supposed to cause "setfacl" to skip over any symbolic links it encounters, did not work as expected: symbolic links were still followed. This update fixes this so that the '-P' flag works as expected and symbolic links are silently skipped over. ([BZ#436070](https://bugzilla.redhat.com/show_bug.cgi?id=436070))<sup>4</sup>

\* the "setfacl" command failed to resolve relative symbolic links when it encountered them unless they were specified with a trailing forward-slash character (in the case of relative symbolic links to directories), or the script or shell prompt's working directory was the directory which contained the relative symbolic link(s). With this update, relative symbolic links are handled correctly by setfacl regardless of where they are encountered or what their target is. ([BZ#500095](https://bugzilla.redhat.com/show_bug.cgi?id=500095))<sup>5</sup>

\* the "getfacl" and "setfacl" commands did not properly handle non-ASCII characters with the result that calling either command on a system with the correct locale settings still produced incorrect output, such as octal character representations. With this update, getfacl and setfacl are now able to produce correct output when using non-ASCII character sets. ([BZ#507747](https://bugzilla.redhat.com/show_bug.cgi?id=507747))<sup>6</sup>

All users of Access Control Lists should upgrade to these updated packages, which resolve this issue.

---

<sup>2</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=368451](https://bugzilla.redhat.com/show_bug.cgi?id=368451)

<sup>3</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=430458](https://bugzilla.redhat.com/show_bug.cgi?id=430458)

<sup>4</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=436070](https://bugzilla.redhat.com/show_bug.cgi?id=436070)

<sup>5</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=500095](https://bugzilla.redhat.com/show_bug.cgi?id=500095)

<sup>6</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=507747](https://bugzilla.redhat.com/show_bug.cgi?id=507747)

### 1.2. acpid

#### 1.2.1. RHBA-2010:0004: bug fix update



##### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2010:0004](#)<sup>7</sup>

An updated acpid package that fixes a bug is now available.

acpid is a daemon that dispatches ACPI (Advanced Configuration and Power Interface) events to user-space programs.

This updated acpid package fixes the following bug:

\* the acpid package that was included with the Red Hat Enterprise Linux 5.4 update contained a package update script that returned a non-zero exit code when the the `/var/log/acpid` log file did not exist. However, if the acpid daemon had never been started on the system, and therefore `/var/log/acpid` did not exist, the faulty check caused the update process to fail, which could have resulted in two different acpid packages being installed on the same system and registered with the RPM database (rpmdb). This updated acpid package removes the spurious record from the rpmdb, thus resolving the problem. ([BZ#548374](#))<sup>8</sup>

All users of acpid are advised to upgrade to this updated package, which resolves this issue.

#### 1.2.2. RHSA-2009:1642: Important security update



##### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2009:1642](#)<sup>9</sup>

An updated acpid package that fixes one security issue is now available for Red Hat Enterprise Linux 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

acpid is a daemon that dispatches ACPI (Advanced Configuration and Power Interface) events to user-space programs.

It was discovered that acpid could create its log file ("`/var/log/acpid`") with random permissions on some systems. A local attacker could use this flaw to escalate their privileges if the log file was created as world-writable and with the `setuid` or `setgid` bit set. ([CVE-2009-4033](#))<sup>10</sup>

Please note that this flaw was due to a Red Hat-specific patch (`acpid-1.0.4-fd.patch`) included in the Red Hat Enterprise Linux 5 acpid package.

---

<sup>8</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=548374](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=548374)

<sup>10</sup> <https://www.redhat.com/security/data/cve/CVE-2009-4033.html>

Users are advised to upgrade to this updated package, which contains a backported patch to correct this issue.

## 1.3. aide

### 1.3.1. RHBA-2010:0036: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2010:0036](#)<sup>11</sup>

An updated aide package that allows proper operation with the recently updated version of libgcrypt and makes minor man page changes is now available.

Advanced Intrusion Detection Environment (AIDE) is a program that creates a database of files on a system, and then uses that database to ensure file integrity and detect system intrusions.

This updated aide package includes the following fixes:

\* the current version of libgcrypt includes a version-checking initialization step that aide was not doing. Running "aide -i" logged the following message to `/var/log/messages`:

```
aide: Libgcrypt warning: missing initialization - please fix the application
```

With this update, aide now includes the version-checking step required by libgcrypt and the libgcrypt warning is, consequently, no longer written to `/var/log/messages`. Note: although based on a proposed upstream patch, this update leaves secure memory enabled, unlike the proposed upstream change. ([BZ#530485](#)<sup>12</sup>)

\* the FILES section of the aide man page previously listed the locations for `aide.conf`, `aide.db.gz` and `aide.db.new.gz` with a pre-pended "%prefix" variable. The updated aide man page removes this variable, listing the file locations as complete but plain paths (eg `/etc/aide.conf`). (No BZ#)

All aide users are advised to upgrade to this updated package, which includes this bug fix and man page change.

## 1.4. anaconda

### 1.4.1. RHBA-2010:0194: bug fix and enhancement update

**Anaconda** is the system installer.

This updated **anaconda** package provides fixes for the following bugs:

- previously, when **anaconda** could not read the *extended display identification data* (EDID) of a monitor, it reverted to text mode. However, EDID information is frequently not available on systems connected to *Keyboard–Video–Mouse* (KVM) switches. Therefore, when installing Red Hat Enterprise Linux 5 on a system with a KVM switch, installation would be constrained to text mode. **Anaconda** no longer checks for bad or missing EDID, and allows graphical installation to proceed

<sup>12</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=530485](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=530485)

even when this information is unavailable. Graphical installation on machines attached to KVM switches therefore continues as if them monitor were connected directly to the graphics adapter. ([BZ#445486](#)<sup>13</sup>)

- previously, **anaconda** expected storage devices to be available immediately when it probed for the location of a kickstart file. On systems where USB storage might not be available immediately (for example, IBM BladeCenter systems), **anaconda** would not find the kickstart file and would prompt the user for its location. This interaction negated the usefulness of kickstart, since the installation could not then complete unattended. **Anaconda** now waits until it has probed five times or for more than 31 seconds before prompting the user for the location of a kickstart file. This allows USB storage enough time to respond and for kickstart to proceed unattended. ([BZ#460566](#)<sup>14</sup>)
- previously, some user interface elements in the the Malayalam translation of **anaconda** overlapped. The overlapping elements disabled some buttons in the screen where **anaconda** lets users to choose a partitioning scheme for the system, and prevented installation from continuing. The text of the Malayalam translation has been shortened so that the interface elements no longer overlap. The buttons on the partitioning scheme screen now work correctly and allow installation to continue. ([BZ#479353](#)<sup>15</sup>)
- during installation, **anaconda** automatically examines any storage device that has the label **OEMDRV** for driver updates and applies any updates that it finds there. Previously, **anaconda** searched for this label on the devices listed in **/proc/partitions**. However, **/proc/partitions** does not identify CD or DVD media, so **anaconda** overlooked optical disks that had the correct label. **Anaconda** now examines the devices listed in **/sys/block**. Therefore, **anaconda** correctly identifies CDs and DVDs labelled **OEMDRV** as driver discs and automatically applies any driver updates contained on them. ([BZ#485060](#)<sup>16</sup>)
- previously, if **anaconda** required network access early in an installation (for example, to retrieve a kickstart file or driver disk image), it temporarily saved information about the network configuration while it enabled access to the network. However, if **anaconda** required network access again for a separate reason, it would not attempt to configure network access again, but would not be able to connect to the network either, because it no longer retained the configuration information that it had already used. Therefore, **anaconda** could not download both a kickstart file and a driver disk image over a network. **Anaconda** now retains the network configuration that it obtains early in the installation process, and can reuse this information multiple times. Therefore, **anaconda** can use more than one resource obtained over a network during installation. ([BZ#495042](#)<sup>17</sup>)
- previously, while upgrading a system, **anaconda** did not check whether packages marked for installation as dependencies were already installed on the system. Consequently, many packages would be reinstalled during an upgrade, wasting time and, in the case of network installations, bandwidth. Now, when performing an upgrade, **anaconda** matches the packages to be installed against the packages that are already installed. Any packages with the same *Name*, *Arch*, *Epoch*, *Version*, *Release* (NAEVR) as a package already on the system are skipped and not reinstalled. ([BZ#495796](#)<sup>18</sup>)
- previously, **anaconda** did not specify a value for **HOTPLUG** when writing the system's networking configuration files, although it did write a value for **ONBOOT**. Because **HOTPLUG** is enabled by default, the effect of disabling **ONBOOT** was limited because any interface not activated at boot time would be enabled anyway whenever probed by the system. **Anaconda** now writes a value for **HOTPLUG**, setting it to the same value as **ONBOOT**. Therefore, any network interface not meant to be enabled at boot time will not be automatically enabled by probing either. ([BZ#498086](#)<sup>19</sup>)

- the **part** kickstart command accepts an option called **--label** that allows a label to be applied to a disk partition during a kickstart installation. However, the code that implemented this option was previously missing from **anaconda**. Any label specified in a kickstart file was therefore ignored. **Anaconda** now includes code to transfer the specified label from the kickstart file to the disk partition. Users can now label disk partitions during kickstart installations. ([BZ#498856](#)<sup>20</sup>)
- when running in rescue mode, **anaconda** previously lacked the ability to identify partitions on logical volumes if the partitions were identified in `fstab` by label rather than by device name. Therefore, if the root (`/`) partition were identified in this way, the usefulness of rescue mode would be limited. **Anaconda** in rescue mode now uses the `getLabels()` method to find partitions and therefore properly detects root partition even if it resides on a logical volume and is identified by label in `fstab`. ([BZ#502178](#)<sup>21</sup>)
- previously, the help text available while configuring `NETTYPE` for IBM System z systems did not mention HiperSockets. Users new to System z might therefore not have known to choose **qeth** to configure HiperSocket interfaces on their hardware. The help text has now been updated to indicate the correct choice and users can select the appropriate option. ([BZ#511962](#)<sup>22</sup>)
- when the `RUNKS` was set to `0` in the `CMSCONFFILE` file on IBM System z systems, **anaconda** should have performed an installation in interactive mode. However, a rewrite of `linuxrc.s390` changed the behavior of `RUNKS` and led to **anaconda** ignoring this variable. Installation would therefore proceed in non-interactive mode regardless of what value was set in `CMSCONFFILE`. A new test is now included in the version of `linuxrc.s390` in Red Hat Enterprise Linux 5.5 so that **anaconda** honors `RUNKS=0` and performs an interactive install if this value is set. ([BZ#513951](#)<sup>23</sup>)
- by design, **anaconda** recognizes any block device with the label `OEMDRV` as a driver disc and searches it for a driver update. However, **anaconda** previously failed to examine dev nodes and therefore, it would not recognize this label on USB storage devices mounted as a partitionless block devices. **Anaconda** now examines dev nodes for the label `OEMDRV` and treats them the same as partitions with this label. It is therefore possible to use a partitionless device as a driver disc. ([BZ#515437](#)<sup>24</sup>)
- previously, **anaconda** did not reinitialize its record of the partition layout on a system when users clicked the **back** button from the partitioning screen. Therefore, when a user selected a partition layout, went back to an earlier screen, and then went forward again to choose a different partition layout, **anaconda** would attempt to implement the new partition layout over the previously-selected partition layout instead of the partition layout actually present on the system. This would sometimes result in a crash. Now, when users step backwards from the partitioning screen, **anaconda** reinitializes its record of the partitions present on the system. Users can therefore change their minds about partitioning options without crashing **anaconda**. ([BZ#516715](#)<sup>25</sup>)
- systems store information about iSCSI targets to which they are connected in the *iSCSI Boot Firmware Table* (iBFT) in BIOS. Previously, however, when **anaconda** installed Red Hat Enterprise Linux 5 from a local installation source such as a CD, DVD, or hard disk, it would not initialize network connections before asking users to configure storage on the system. Therefore, on systems with iSCSI storage, users would have to configure a network connection manually before proceeding with installation, even when this information was already available to **anaconda** in the system BIOS. Now, when **anaconda** detects a valid iBFT present on a system, it automatically loads the network configuration specified there and does not require users to enter this information. Installation from local media on systems with iSCSI storage is therefore simpler and more reliable. ([BZ#517768](#)<sup>26</sup>)
- due to faulty logic, **anaconda** previously did not parse IPv6 addresses correctly and attempted to read the final byte of the address as a port number. It was therefore not possible, for example,

to install on an iSCSI target specified by in IPv6 address. The logic by which **anaconda** parses IP addresses has now been corrected, but now requires IPv6 addresses to be specified in the **[address]:port** form to comply with the relevant RFCs. This form removes ambiguity, since IPv6 addresses are still valid if they omit a sequence of bytes with zero values. When IPv6 addresses are specified in this format, **anaconda** parses them correctly and installation continues as normal. ([BZ#525054](#)<sup>27</sup>)

- comments in kickstart files are marked with a pound symbol (#) at the start of the line. However, **anaconda** did not previously account for the possibility that users might mark a comment with multiple pound symbols (for example, #####). **Anaconda** would therefore attempt to parse lines that started with multiple pound symbols and installation would fail. **Anaconda** now recognizes lines that start with multiple pound symbols as comments and does not attempt to parse them. Users can now safely mark comments in kickstart files in this way. ([BZ#525676](#)<sup>28</sup>)
- to avoid a circular dependency that exists between the *ghostscript* and *ghostscript-fonts* packages, **anaconda** ignored *ghostscript*'s dependency on *ghostscript-fonts*. However, *ghostscript-fonts* was not explicitly installed as part of the **Printing** package group. The usefulness of **Ghostscript** as installed by **anaconda** was therefore limited. **Anaconda** still avoids the circular dependency, but now specifically installs *ghostscript-fonts* when users select the **Printing** package group. ([BZ#530548](#)<sup>29</sup>)
- previously, **anaconda** did not automatically instruct the kernel to check for multipath devices when installing on IBM System z systems. Therefore, unless users booted with the **mpath** boot option, iSCSI devices detected on more than one path would be represented in the installer multiple times, one for each path. **Anaconda** now automatically loads the **mpath** boot option and therefore represents multipath devices correctly. ([BZ#538129](#)<sup>30</sup>)
- Dell PowerEdge servers equipped with the SAS6i/R integrated RAID controller use *BIOS Enhanced Disk Drive Services* (EDD) to identify the storage device from which to boot the operating system. Previously, **anaconda** did not parse EDD to identify the correct boot device. Consequently, with a RAID 0 and RAID 1 configured on the system, **anaconda** would choose the wrong device and the system would not be bootable. **Anaconda** now parses EDD to support the SAS6i/R integrated RAID controller, so that it selects the correct boot device for systems that use this device. ([BZ#540637](#)<sup>31</sup>)
- previously, **anaconda** would always attempt to reconstruct pre-existing *Logical Volume Management* (LVM) devices during installation. **Anaconda** would attempt to recreate the LVM device even when a user cleared the LVM partitions from one or more of the disks that held partitions that formed part of a volume group. In this case, installation would fail. Now, **anaconda** no longer attempts to reconstruct incomplete LVM devices. Users can therefore safely re-allocate storage that was once part of a volume group and installation will proceed as expected. ([BZ#545869](#)<sup>32</sup>)
- when **ksdevice=link** is set in a kickstart file, **anaconda** should automatically select the first available network interface and use it during installation. This avoids the need for user input and allows installation to proceed unattended. However, if interfaces were in a state where **anaconda** could not determine their status, **anaconda** would revert to interactive mode and prompt the user to select a network interface, thus making unattended installation impossible on systems where network interfaces could be in such a state. **Anaconda** now forces the network interfaces on the system into **IFF\_UP** and **IFF\_RUNNING** states before it attempts to obtain link status. Because the interfaces are now in a state where they can report their link status to **anaconda**, **Anaconda** can automatically choose one to use during installation and kickstart installations can proceed unattended. ([BZ#549751](#)<sup>33</sup>)



- previously, when installing on IBM System z systems, **anaconda** assumed that the network gateway was unreachable if its attempt to ping the gateway timed out after 10 seconds. **Anaconda** would then prompt the user to select a gateway. However, if **IPADDR** in the **conf** file has changed recently, network interfaces take longer to respond. **Anaconda** now prompts the user only when three pings have failed and therefore avoids prompting the user for gateway information that is already correctly specified in the **conf** file. ([BZ#506742](#)<sup>34</sup>)

In addition, this updated package provides the following enhancements:

- after transferring installation files to a z/VM guest, a user must execute a series of *Conversational Monitor System* (CMS) commands to IPL the zLinux installation. These commands can be scripted, but no such script was previously included with Red Hat Enterprise Linux 5. The lack of a readymade script made installation more difficult for users unfamiliar with CMS commands. The CMS script for starting the install process on z/VM is now included in the Red Hat Enterprise Linux 5 images, simplifying installation. ([BZ#475343](#)<sup>35</sup>)
- **anaconda** now loads the Brocade BNA Ethernet Controller driver, and supports Brocade Fibre Channel to PCIe Host Bus Adapters. ([BZ#475707](#)<sup>36</sup>)
- previously, **anaconda** did not offer users the opportunity to configure NFS options during interactive installation (although these could be configured in kickstart files). Users who needed to fine-tune NFS parameters for installation were therefore forced to run an unattended installation. Now, **anaconda** presents users who select NFS installation with a dialog in which they can configure NFS options to suit their needs. ([BZ#493052](#)<sup>37</sup>)
- previously, it was not possible to configure hypervisor parameters during a kickstart installation. As a result, users needed to specify hypervisor parameters manually after installation, negating the usefulness of kickstart as a mechanism for unattended installations. Now, **anaconda** recognizes a new kickstart option, **--hvargs** and sets Hypervisor parameters accordingly. ([BZ#501438](#)<sup>38</sup>)
- previously, during a kickstart installation when multiple multipath LUNs were available, **anaconda** would automatically choose the LUN with the lowest ID number for the root device. Users had no ready way to customize this behavior. Now, **anaconda** supports a **multipath** kickstart command with **--name** and **--device** options that allow users to specify a LUN for root. ([BZ#502768](#)<sup>39</sup>)
- **anaconda** can retrieve kickstart files from FTP servers. Previously, however, **anaconda** did not support users specifying authentication credentials to access an FTP server. Therefore, if access to the server were protected by a passphrase, **anaconda** could not retrieve the kickstart file. Now, when specifying the location of a kickstart file with the **ks=** boot option, users can provide a passphrase to allow **anaconda** to retrieve the kickstart files from a protected server. ([BZ#505424](#)<sup>40</sup>)
- previously, troubleshooting errors that occurred while running **%pre** and **%post** kickstart scriptlets was very difficult because **anaconda** did not log the behavior of these scriptlets. **Anaconda** now copies **%pre** and **%post** kickstart scriptlets to **/tmp** together with a log. These records make troubleshooting kickstart installations easier. ([BZ#510636](#)<sup>41</sup>)
- **Reipl** is a kernel feature that instructs IBM System z systems where to boot next, as these systems do not have a default boot location. **Anaconda** did not previously support **Reipl**, which meant that during installation, users had to specify a boot location manually between different phases of the installation. **Anaconda** now supports **Reipl**, so these reboots can happen automatically. ([BZ#512195](#)<sup>42</sup>)

- *NPort ID Virtualization* (NPIV) presents one physical Fibre Channel adapter port to the SAN as multiple WWNN/WWPN pairs. **Anaconda** now supports NPIV, which allows users on PowerPC systems to install to a NPIV LUN. ([BZ#512237](#)<sup>43</sup>)
- the Python executables that make up **anaconda** now all explicitly use the system Python (`#!/usr/bin/python` instead of `#!/usr/bin/env python`). This ensures that **anaconda** functions correctly when more than one Python stack is present on a system. ([BZ#521337](#)<sup>44</sup>)
- **anaconda** now supports the Emulex OneConnect iSCSI network interface card. ([BZ#529442](#)<sup>45</sup>)
- **anaconda** now supports PMC Sierra MaxRAID controller adapters. ([BZ#532777](#)<sup>46</sup>)
- although users have been able to specify package groups for installation in kickstart files, using the @ prefix, it was not possible to exclude package groups from installation, only individual packages. **Anaconda** now supports excluding package groups with the -@ prefix ([BZ#558516](#)<sup>47</sup>)
- **anaconda** now loads the **xorg-x11-qxl-drv** and **xorg-x11-ast-drv** X11 video drivers as required. **xorg-x11-qxl-drv** supports the qemu QXL video accelerator when installing Red Hat Enterprise Linux 5 as a guest operating system. **xorg-x11-ast-drv** supports ASPEED Technologies video hardware. ([BZ#567666](#)<sup>48</sup>)

## 1.5. apr-util

### 1.5.1. RHEA-2010:0310: enhancement update

Updated apr-util packages that add support for MySQL are now available.

apr-util is a utility library used with the Apache Portable Runtime (APR). It aims to provide a free library of C data structures and routines. This library contains additional utility interfaces for APR; including support for XML, LDAP, database interfaces, URI parsing, and more.

In previous releases, the APR utility library DBD (database abstraction) interface did not include support for MySQL databases. This update adds the MySQL driver to the DBD interface. ([BZ#252073](#)<sup>49</sup>, [BZ#491342](#)<sup>50</sup>)

All users requiring MySQL support should install these newly released packages, which add this enhancement.

## 1.6. at

### 1.6.1. RHBA-2009:1654: bug fix and enhancement update



#### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2009:1654](#)<sup>51</sup>

---

<sup>49</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=252073](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=252073)

<sup>50</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=491342](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=491342)

---

An updated "at" package that adds and documents a configuration enhancement and corrects the -debuginfo build is now available.

"At" and "Batch" read commands from standard input or from a specified file. At allows you to specify that a command will be run at a particular time. Batch will execute commands when the system load levels drop to a particular level. Both commands use /bin/sh.

This update addresses the following issue:

\* although "at" contains ELF objects, the at-debuginfo package was empty. With this update the -debuginfo package contains valid debugging information as expected. ([BZ#500542](https://bugzilla.redhat.com/show_bug.cgi?id=500542)<sup>52</sup>)

This update also adds the following enhancements:

\* previously, the atd daemon ran with hard-coded options and could only be configured at the command-line. The atd daemon now reads a configuration file, /etc/sysconfig/atd, when it starts up, enabling easier configuration, particularly for load options and multiprocessor systems. ([BZ#232259](https://bugzilla.redhat.com/show_bug.cgi?id=232259)<sup>53</sup>)

\* The DESCRIPTION section of the "at" man page has been updated to note the existence, location and purpose of the /etc/sysconfig/atd configuration file. Note: as the man page suggests, the sample configuration file included with this update is the primary source of information about atd configuration options. ([BZ#537792](https://bugzilla.redhat.com/show_bug.cgi?id=537792)<sup>54</sup>)

Users are advised to upgrade to this updated package, which fixes this bug and adds these enhancements.

## 1.7. audit

### 1.7.1. RHBA-2010:0228: bug fix update

An updated audit package that fixes various bugs and provides an enhancement is now available.

The audit package contains the user space utilities for storing and searching the audit records generate by the audit subsystem in the Linux 2.6 kernel.

This update includes the following fixes:

\* The man page was ambiguous in explaining the structure of dates and the supplied examples often did not work because of different date formats in various locales. This caused some confusion amongst users. The page has been rewritten to clarify that the date format accepted by aureport and ausearch is influenced by the LC\_TIME environmental variable, eliminating the confusion about this issue. ([BZ#513974](https://bugzilla.redhat.com/show_bug.cgi?id=513974)<sup>55</sup>)

\* The audit package's libauparse function had a bug that meant it could not interpret IPC (inter-process communication) mode fields. When it attempted to do so, a segmentation fault would occur. The audit package has now been patched so that IPC mode fields are interpreted by the software without crashes resulting. ([BZ#519790](https://bugzilla.redhat.com/show_bug.cgi?id=519790)<sup>56</sup>)

This update also includes the following enhancement:

---

<sup>52</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=500542](https://bugzilla.redhat.com/show_bug.cgi?id=500542)

<sup>53</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=232259](https://bugzilla.redhat.com/show_bug.cgi?id=232259)

<sup>54</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=537792](https://bugzilla.redhat.com/show_bug.cgi?id=537792)

<sup>55</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=513974](https://bugzilla.redhat.com/show_bug.cgi?id=513974)

<sup>56</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=519790](https://bugzilla.redhat.com/show_bug.cgi?id=519790)

\* The audit package has been rebased and, as a result, a number of new features have been added. These include:

1. Allowing ausearch/report to specify multiple node names (which are needed for remote logging).
2. auparse can now handle empty AUSOURCE\_FILE\_ARRAYs.
3. auditctl rules now allow a0-a3 to be negative numbers.
4. An audit.rules man page has been added.
5. auditd resets syslog warnings if disk space becomes available.
6. The != operator in audit\_rule\_fieldpair\_data is now checked.
7. A tcp\_max\_per\_addr option has been added to auditd.conf in order to limit concurrent connections.
8. Many improvements to remote logging code.

As a result, these enhancements are now available for system administrators, making auditing options much more flexible. ([BZ#529851](#)<sup>57</sup>)

## 1.8. autofs

### 1.8.1. RHBA-2009:1468: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1468](#)<sup>58</sup>

An updated autofs package that fixes two bugs is now available.

The autofs utility controls the operation of the automount daemon. The automount daemon automatically mounts file systems when you use them, and unmounts them when they are not busy.

This updated package fixes the following two autofs bugs:

\* autofs was incorrectly using a non-thread-safe libxml2 function as though it was thread-safe. This sometimes resulted in autofs crashing. With this update the calls to xmlCleanupParser() and xmlInitParser() have been moved: these functions are now only called as autofs starts and exits, ensuring these libxml2 functions are not called more than once while autofs is running. ([BZ#523188](#)<sup>59</sup>)

\* a recent correction related to autofs master map entry updating introduced a regression whereby it was possible to deadlock when requesting a map re-load when an entry in a direct map had been removed. This update adds a check that ensures such map re-load requests do not cause a deadlock. ([BZ#525431](#)<sup>60</sup>)

All autofs users should install this updated package which addresses these issues.

### 1.8.2. RHBA-2010:0265: bug fix update

The autofs utility controls the operation of the automount daemon. The automount daemon automatically mounts file systems when you use them, and unmounts them when they are not busy.

This updated package fixes the following bugs:

---

<sup>57</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=529851](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=529851)

<sup>59</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=523188](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=523188)

<sup>60</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=525431](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=525431)

- If an included map read failed, autofs returned an error and subsequent master map entries were not read. This update reports the failure in the log but master map reading no longer ceases. ([BZ#506034](#)<sup>61</sup>)
- autofs could segfault if it called **xmlCleanupParser** concurrently from multiple threads, as this function is not re-entrant. autofs has been changed to call this function only once from its main thread, when the application exits. ([BZ#513289](#)<sup>62</sup>)
- autofs could segfault at startup when using LDAP under certain circumstances. autofs would fail to try and retrieve a query dn if:
  - LDAP is being used to store autofs maps *and...*
  - The LDAP schema to be used for the maps is explicitly defined in the autofs configuration *and...*
  - No master map entries exist in LDAP.

This set of conditions would return success instead of failure. This update fixes the get query dn failure. ([BZ#572603](#)<sup>63</sup>)

- If a master map entry is changed in any other way besides the map name (for example, map wide options) the system encountered two application data structures for the "same" map during a map re-read. If the contents of that map has also changed, a deadlock can occur.

Having the duplicate data structure also caused entries in the problem map to be unmounted. Since direct mount maps have a distinct autofs mount for each entry direct mount they appeared to stop working. This update corrects this behaviour. ([BZ#514412](#)<sup>64</sup>)

- autofs would block for several minutes when attempting to mount from a server that was not available. A new mount\_wait parameter has been added to prevent this block. This update requires SELinux policy 255 or later. ([BZ#517349](#)<sup>65</sup>)
- The autofs parser objected to locations containing the characters '@' and '#' (Lustre and sshfs mounts) causing the mount request to fail. This update allows autofs to parse these characters and mount successfully. ([BZ#520745](#)<sup>66</sup>)
- Due to an incorrect system call an error message stating "Operation not permitted" would be returned when attempting to mount an unknown hostname. This call has been corrected and autofs now returns "hostname lookup failed" as would be expected. ([BZ#533323](#)<sup>67</sup>)
- A typing error in the usage text of the autofs service script has been corrected. ([BZ#534012](#)<sup>68</sup>)
- When changing the timed wait from using select(2) to poll(2) in the non-blocking TCP connection function, to overcome the 1024 file handle limit of select(2), the wait timeout was not correctly converted from seconds to milliseconds. This update corrects the problem. ([BZ#539747](#)<sup>69</sup>)
- autofs failed to mount locations whose path depended on another local auto-mounted mount. Dependent mounts are triggered by calling access(2) on the mount location path prior to mounting the location. The check for whether a location was a local path was restrictive and didn't cater for all cases. This has now been fixed. ([BZ#537403](#)<sup>70</sup>)
- Inter-operability between autofs and some non-open source LDAP servers was impaired when a SASL authenticated connection was used over multiple bind and unbind operations. autofs has been updated use distinct authentication connection for each server it binds to. ([BZ#537793](#)<sup>71</sup>)

- autofs failed to load its maps if all LDAP servers were down, or unreachable, when the daemon started. The dependency on an LDAP server being available at startup has been removed. This change resolved the issue of the map server being unreachable for some common usage cases. ([BZ#543554](#)<sup>72</sup>)
- The random selection option used with mount locations that have multiple servers was not being set correctly during the parsing of master map entries. If specified as a mount option in master map entries the option is now used as has been requested. ([BZ#548476](#)<sup>73</sup>)
- Setting the expire timeout to 0 was causing autofs to constantly schedule expire runs leading to excessive resource usage and premature unmounting of mounts. Setting the timeout to 0 should in fact disable expiry of mounts and this update fixes this incorrect behavior. ([BZ#548277](#)<sup>74</sup>)
- autofs would abort when using DIGEST-MD5 authentication under heavy concurrent access. This was caused by autofs not providing the locking functions required by the cyrus-sasl library. In addition the cyrus-sasl library locking functions contained a race which sometimes lead to a deadlock. This update adds the needed locking functions to autofs and passes them to cyrus-sasl at initialization. The bug in the cyrus-sasl library is fixed in cyrus-sasl-lib 2.1.22-5.el5.el5\_4.3 and later which is required for the update to install if cyrus-sasl is also installed. ([BZ#559430](#)<sup>75</sup>)

All autofs users should upgrade to this updated package, which resolves these issues.

## 1.9. automake

### 1.9.1. RHSA-2010:0321: Low security update

Updated automake, automake14, automake15, automake16, and automake17 packages that fix one security issue are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having low security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

Automake is a tool for automatically generating Makefile.in files compliant with the GNU Coding Standards.

Automake-generated Makefiles made certain directories world-writable when preparing source archives, as was recommended by the GNU Coding Standards. If a malicious, local user could access the directory where a victim was creating distribution archives, they could use this flaw to modify the files being added to those archives. Makefiles generated by these updated automake packages no longer make distribution directories world-writable, as recommended by the updated GNU Coding Standards. ([CVE-2009-4029](#)<sup>76</sup>)

Note: This issue affected Makefile targets used by developers to prepare distribution source archives. Those targets are not used when compiling programs from the source code.

All users of automake, automake14, automake15, automake16, and automake17 should upgrade to these updated packages, which resolve this issue.

---

<sup>76</sup> <https://www.redhat.com/security/data/cve/CVE-2009-4029.html>

## 1.10. avahi

### 1.10.1. RHBA-2010:0034: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2010:0034](#)<sup>77</sup>

Updated avahi packages that address two bugs are now available.

Avahi is an implementation of the DNS Service Discovery and Multicast DNS specifications for Zeroconf Networking. It facilitates service discovery on a local network. Avahi and Avahi-aware applications allow you to plug your computer into a network and, with no configuration, view other people to chat with, see printers to print to, and find shared files on other computers.

This update fixes the following two bugs:

\* previously, avahi published a static SSH-SFTP service by default, regardless of the machine and regardless of whether an ssh server was running or not. As a result, all Red Hat Enterprise Linux instances also running Avahi appeared in the LAN listings of file browsers and file managers (eg "Places > Network" in Nautilus or "Go > Network Folders" in Konquerer) even if they were not acting as file servers. This update still includes a static SSH-SFTP service but it now ships as a deactivated example service (ie, is not published by default). The static SSH-FTP service can be activated manually, but systems running Avahi no longer appear in file manager LAN listings by default. ([BZ#219143](#)<sup>78</sup>)

\* previously, running the Avahi init scripts with a "status" argument resulted in a return code of 0, regardless of whether the daemons are running or not. This update corrects that: a missing avahi daemon now results in a failure return code (1) as expected. ([BZ#232161](#)<sup>79</sup>)

All avahi users should install these updated packages, which address these issues.

## 1.11. bind

### 1.11.1. RHSA-2010:0062: Moderate security update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2010:0062](#)<sup>80</sup>

Updated bind packages that fix two security issues are now available for Red Hat Enterprise Linux 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

<sup>78</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=219143](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=219143)

<sup>79</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=232161](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=232161)



The Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) protocols. BIND includes a DNS server (named); a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating correctly.

A flaw was found in the BIND DNSSEC NSEC/NSEC3 validation code. If BIND was running as a DNSSEC-validating resolver, it could incorrectly cache NXDOMAIN responses, as if they were valid, for records proven by NSEC or NSEC3 to exist. A remote attacker could use this flaw to cause a BIND server to return the bogus, cached NXDOMAIN responses for valid records and prevent users from retrieving those records (denial of service). ([CVE-2010-0097](https://www.redhat.com/security/data/cve/CVE-2010-0097.html)<sup>81</sup>)

The original fix for CVE-2009-4022 was found to be incomplete. BIND was incorrectly caching certain responses without performing proper DNSSEC validation. CNAME and DNAME records could be cached, without proper DNSSEC validation, when received from processing recursive client queries that requested DNSSEC records but indicated that checking should be disabled. A remote attacker could use this flaw to bypass the DNSSEC validation check and perform a cache poisoning attack if the target BIND server was receiving such client queries. ([CVE-2010-0290](https://www.redhat.com/security/data/cve/CVE-2010-0290.html)<sup>82</sup>)

All BIND users are advised to upgrade to these updated packages, which contain a backported patch to resolve these issues. After installing the update, the BIND daemon (named) will be restarted automatically.

### 1.11.2. RHSA-2009:1620: Moderate security update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2009:1620](https://www.redhat.com/security/data/cve/RHSA-2009:1620.html)<sup>83</sup>

Updated bind packages that fix one security issue are now available for Red Hat Enterprise Linux 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) protocols. BIND includes a DNS server (named); a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating correctly.

Michael Sinatra discovered that BIND was incorrectly caching responses without performing proper DNSSEC validation, when those responses were received during the resolution of a recursive client query that requested DNSSEC records but indicated that checking should be disabled. A remote attacker could use this flaw to bypass the DNSSEC validation check and perform a cache poisoning attack if the target BIND server was receiving such client queries. ([CVE-2009-4022](https://www.redhat.com/security/data/cve/CVE-2009-4022.html)<sup>84</sup>)

All BIND users are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing the update, the BIND daemon (named) will be restarted automatically.

---

<sup>81</sup> <https://www.redhat.com/security/data/cve/CVE-2010-0097.html>

<sup>82</sup> <https://www.redhat.com/security/data/cve/CVE-2010-0290.html>

<sup>84</sup> <https://www.redhat.com/security/data/cve/CVE-2009-4022.html>



## 1.12. binutils

### 1.12.1. RHBA-2010:0304: bug fix update

Updated binutils packages that fix various bugs are now available.

Binutils is a collection of binary utilities, including ar (for creating, modifying and extracting from archives), as (a family of GNU assemblers), gprof (for displaying call graph profile data), ld (the GNU linker), nm (for listing symbols from object files), objcopy (for copying and translating object files), objdump (for displaying information from object files), ranlib (for generating an index for the contents of an archive), readelf (for displaying detailed information about binary files), size (for listing the section sizes of an object or archive file), strings (for listing printable strings from files), strip (for discarding symbols), and addr2line (for converting addresses to file and line).

These updated binutils packages provide fixes for the following bugs:

\* The readelf debugging utility was placing subject error messages in the middle of the .debug\_str in the stderr output. This meant that location lists in the .debug\_info section that were not in ascending order could not be handled correctly and the debugger could pick the wrong function, leading to dropped debug information. A patch has now been added and, as a result, the location lists can now be handled correctly, irrespective of order. As a result, the debugger now picks the right function when looking up symbols and debug information is no longer dropped. ([BZ#499164](https://bugzilla.redhat.com/show_bug.cgi?id=499164)<sup>85</sup>,

[BZ#509124](https://bugzilla.redhat.com/show_bug.cgi?id=509124)<sup>86</sup>)

\* The strings command was not parsing files correctly. When used with a multi-digit <NUM> argument (such as strings -10 filename.txt) an "invalid integer argument" error would occur because it regarded each numeral as a separate argument. The parsing has now been corrected via a patch to strings.c.multidigit\_input so that multi-digit numerals are regarded as parts of a single argument. As a result, files are now parsed correctly. ([BZ#508765](https://bugzilla.redhat.com/show_bug.cgi?id=508765)<sup>87</sup>)

\* There was a regression in binutils-devel that caused it to build "oprofile" files incorrectly. As a result, bfd\_get\_section\_by\_name() returned incorrect information about the debuginfo section and an "opreport" error would occur. The bfd.h header's API has now been fixed to match the BFD library's ABI. As a result, the per-symbol profile is now generated correctly and the opreport runs without error. ([BZ#529028](https://bugzilla.redhat.com/show_bug.cgi?id=529028)<sup>88</sup>)

\* There was a link failure whereby when a symbol in a comdat/linkonce section had a different level of visibility in different files, the linker could not merge the visibility. As a consequence, after the ld command was run, a "final link failed: Bad value" error would occur. A patch has been added to elflink.c.sym\_visibility to make sure that the visibility is kept. As a result, ld now can now merge different levels of visibility without error. ([BZ#531269](https://bugzilla.redhat.com/show_bug.cgi?id=531269)<sup>89</sup>)

Users are advised to upgrade to these updated binutils packages, which resolve these issues.

---

<sup>85</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=499164](https://bugzilla.redhat.com/show_bug.cgi?id=499164)

<sup>86</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=509124](https://bugzilla.redhat.com/show_bug.cgi?id=509124)

<sup>87</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=508765](https://bugzilla.redhat.com/show_bug.cgi?id=508765)

<sup>88</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=529028](https://bugzilla.redhat.com/show_bug.cgi?id=529028)

<sup>89</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=531269](https://bugzilla.redhat.com/show_bug.cgi?id=531269)

### 1.13. bogl

#### 1.13.1. RHBA-2009:1593: bug fix update



##### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2009:1593](#)<sup>90</sup>

Updated bogl packages that fix a bug are now available.

Ben's Own Graphics Library (BOGL) is a small graphics library for Linux kernel frame buffers. It supports only very simple graphics. The bogl packages also include bterm, a Unicode-capable terminal program for the Linux frame buffer.

These updated packages provide a fix for the following bug:

\* when editing a file with vi from within the bterm console, a SIGSEGV error could occur, causing both vi and bterm to crash. This update adds a check that keeps "yorig" from equaling -1, which prevents the underlying memory reference error occurring. ([BZ#517957](#)<sup>91</sup>)

All bogl users are advised to upgrade to these updated packages, which resolve this issue.

### 1.14. bootparamd

#### 1.14.1. RHBA-2010:0057: bug fix update



##### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2010:0057](#)<sup>92</sup>

An updated bootparamd package that fixes a bug is now available.

Bootparamd is a server process that provides information to diskless clients necessary for booting; consulting the /etc/bootparams file for required information.

When bootparamd is used for multihomed environment handling, it would previously evaluate the route to be returned to the first requesting client and re-evaluate the route to be returned for each client thereafter. Even though it re-evaluates what router IP to return for each following client, it would always send back the first route, due to it being the one that was cached. This updated package ensures that no re-evaluation occurs concerning the router IP to return for each client. ([BZ#446108](#)<sup>93</sup>)

All users of bootparamd are advised to upgrade to this updated package, which resolves this issue.

---

<sup>91</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=517957](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=517957)

<sup>93</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=446108](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=446108)

## 1.15. booty

### 1.15.1. RHBA-2010:0185: bug fix and enhancement update

An updated booty package that fixes a bug and adds an enhancement is now available.

The booty package contains a python library which provides an interface for the creation of boot loader configuration files and the addition of stanzas to said configuration files. These boot loader configuration files are used by the anaconda installer.

This updated booty package fixes the following bug:

\* early in the installation process, anaconda creates a ramdisk to hold files that it will need to complete the installation. Previously, when installing the debug kernel for Red Hat Enterprise Linux on IBM System z, the ramdisk was larger than the default memory address that ZIPL allocated to hold the ramdisk. Installation would therefore fail. The `/etc/zipl.conf` file that booty creates for anaconda now explicitly specifies a suitable address for the ramdisk so that ZIPL does not rely on the insufficient default address. With enough space to create the ramdisk, installation succeeds. ([BZ#429906](https://bugzilla.redhat.com/show_bug.cgi?id=429906)<sup>94</sup>)

In addition, this updated package provides the following enhancement:

\* previously, there was no way to configure hypervisor parameters during a kickstart installation. Therefore, these parameters would have to be configured manually after installation. Red Hat Enterprise Linux now includes a new option for the "bootloader" command in kickstart, "--hvargs", which sets hypervisor parameters in `grub.conf` during installation. It is now possible to automate this part of the installation process. Refer to the Red Hat Enterprise Linux 5 Installation Guide for a description of the "--hvargs" option. ([BZ#552957](https://bugzilla.redhat.com/show_bug.cgi?id=552957)<sup>95</sup>)

Users of booty are advised to upgrade to this updated booty package, which resolves this issue and adds this enhancement.

## 1.16. brlTTY

### 1.16.1. RHSA-2010:0181: Low security and bug fix update

Updated brlTTY packages that fix one security issue and several bugs are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having low security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

brlTTY (Braille TTY) is a background process (daemon) which provides access to the Linux console (when in text mode) for a blind person using a refreshable braille display. It drives the braille display, and provides complete screen review functionality.

It was discovered that a brlTTY library had an insecure relative RPATH (runtime library search path) set in the ELF (Executable and Linking Format) header. A local user able to convince another user

<sup>94</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=429906](https://bugzilla.redhat.com/show_bug.cgi?id=429906)

<sup>95</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=552957](https://bugzilla.redhat.com/show_bug.cgi?id=552957)

to run an application using brltty in an attacker-controlled directory, could run arbitrary code with the privileges of the victim. ([CVE-2008-3279](https://www.redhat.com/security/data/cve/CVE-2008-3279.html)<sup>96</sup>)

These updated packages also provide fixes for the following bugs:

- \* the brltty configuration file is documented in the brltty manual page, but there is no separate manual page for the /etc/brltty.conf configuration file: running "man brltty.conf" returned "No manual entry for brltty.conf" rather than opening the brltty manual entry. This update adds brltty.conf.5 as an alias to the brltty manual page. Consequently, running "man brltty.conf" now opens the manual entry documenting the brltty.conf specification. ([BZ#530554](https://bugzilla.redhat.com/show_bug.cgi?id=530554)<sup>9897</sup>)

- \* previously, the brltty-pm.conf configuration file was installed in the /etc/brltty/ directory. This file, which configures Papeermeier Braille Terminals for use with Red Hat Enterprise Linux, is optional. As well, it did not come with a corresponding manual page. With this update, the file has been moved to /usr/share/doc/brltty-3.7.2/BrailleDrivers/Papeermeier/. This directory also includes a README document that explains the file's purpose and format. ([BZ#530554](https://bugzilla.redhat.com/show_bug.cgi?id=530554)<sup>10099</sup>)

- \* during the brltty packages installation, the message

Creating screen inspection device /dev/vcsa...done.

was presented at the console. This was inadequate, especially during the initial install of the system. These updated packages do not send any message to the console during installation. ([BZ#529163](https://bugzilla.redhat.com/show_bug.cgi?id=529163)<sup>101</sup>)

- \* although brltty contains ELF objects, the brltty-debuginfo package was empty. With this update, the -debuginfo package contains valid debugging information as expected. ([BZ#500545](https://bugzilla.redhat.com/show_bug.cgi?id=500545)<sup>102</sup>)

- \* the MAX\_NR\_CONSOLES definition was acquired by brltty by #including linux/tty.h in Programs/api\_client.c. MAX\_NR\_CONSOLES has since moved to linux/vt.h but the #include in api\_client.c was not updated. Consequently, brltty could not be built from the source RPM against the Red Hat Enterprise Linux 5 kernel. This update corrects the #include in api\_client.c to linux/vt.h and brltty now builds from source as expected. ([BZ#456247](https://bugzilla.redhat.com/show_bug.cgi?id=456247)<sup>103</sup>)

All brltty users are advised to upgrade to these updated packages, which resolve these issues.

## 1.17. checkpolicy

### 1.17.1. RHBA-2010:0184: bug fix update

An updated checkpolicy package that makes a man page correction, fixes help message and man page omissions and allows the unknown access flag to be specified is now available.

checkpolicy is the policy compiler for Security-Enhanced Linux (SELinux). The checkpolicy utility is required for building SELinux policies.

This updated checkpolicy package addresses the following issues:

---

<sup>96</sup> <https://www.redhat.com/security/data/cve/CVE-2008-3279.html>

<sup>98</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=530554](https://bugzilla.redhat.com/show_bug.cgi?id=530554)

<sup>97</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=530554](https://bugzilla.redhat.com/show_bug.cgi?id=530554)

<sup>100</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=530554](https://bugzilla.redhat.com/show_bug.cgi?id=530554)

<sup>99</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=530554](https://bugzilla.redhat.com/show_bug.cgi?id=530554)

<sup>101</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=529163](https://bugzilla.redhat.com/show_bug.cgi?id=529163)

<sup>102</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=500545](https://bugzilla.redhat.com/show_bug.cgi?id=500545)

<sup>103</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=456247](https://bugzilla.redhat.com/show_bug.cgi?id=456247)

\* newer SELinux kernels have access checks that the shipping SELinux policy package does not understand. The kernel currently denies these access checks by default. This updated checkpolicy package can build an selinux-policy package that tells the kernel to "Allow" unknown access. ([BZ#531229](https://bugzilla.redhat.com/show_bug.cgi?id=531229)<sup>104</sup>)

\* the checkpolicy man page listed (but did not otherwise document) a "-m" switch. checkpolicy supports a "-M" switch but not a "-m" switch. This update removes the "-m" option from the checkpolicy SYNOPSIS. Note: the "-M" switch was and is documented in the OPTIONS section of the checkpolicy man page. ([BZ#533790](https://bugzilla.redhat.com/show_bug.cgi?id=533790)<sup>105</sup>)

\* checkmodule's "-d" switch (which switches the tool to debug mode) was documented in the checkmodule man page but not in the output of checkmodule's help message (ie the output of "checkmodule --help" or "checkmodule -h"). Also, the "-h" switch was not documented at all. With this update, the "-d" switch is now included in help message output and the "-h" switch is documented in both the checkmodule man page and the checkmodule help message. ([BZ#533796](https://bugzilla.redhat.com/show_bug.cgi?id=533796)<sup>106</sup>)

All SELinux users should install this updated package which resolves these issues.

## 1.18. chkconfig

### 1.18.1. RHBA-2009:1628: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2009:1628](https://errata.redhat.com/RHBA-2009:1628)<sup>107</sup>

Updated chkconfig packages that resolve several issues with the alternatives utility and provide various man page corrections are now available.

The basic system utility chkconfig updates and queries runlevel information for system services.

These updated chkconfig packages provide fixes for the following bugs:

\* when the "alternatives" utility was run and an error occurred, no contextual information such as the line number of the error was provided. With this update, upon an error, "alternatives" now provides the line number where the error occurred in the relevant file in the `/var/lib/alternatives` directory, which helps to diagnose alternatives-related errors. ([BZ#441443](https://bugzilla.redhat.com/show_bug.cgi?id=441443)<sup>108</sup>)

\* using the "alternatives" utility and selecting the last available option and then uninstalling the program which provided that alternative did not result in the removal of the symbolic links for that option. Because the previously-set alternative was no longer available and the symbolic link remained, the program was then rendered unusable. With this update, when the aforementioned condition is met, the "alternatives" program now recognizes that the program is no longer available and removes the extraneous symbolic link, with the result that the next-best alternative is properly selected, and running the program works as expected. ([BZ#525051](https://bugzilla.redhat.com/show_bug.cgi?id=525051)<sup>109</sup>)

<sup>104</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=531229](https://bugzilla.redhat.com/show_bug.cgi?id=531229)

<sup>105</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=533790](https://bugzilla.redhat.com/show_bug.cgi?id=533790)

<sup>106</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=533796](https://bugzilla.redhat.com/show_bug.cgi?id=533796)

<sup>108</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=441443](https://bugzilla.redhat.com/show_bug.cgi?id=441443)

<sup>109</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=525051](https://bugzilla.redhat.com/show_bug.cgi?id=525051)

\* the `chkconfig(8)` man page contained a description of the syntax for running `chkconfig` that differed from the correct description presented when running "`chkconfig --help`". The man page has been corrected to correspond with the program's help information. ([BZ#501225](https://bugzilla.redhat.com/show_bug.cgi?id=501225)<sup>110</sup>)

\* the `chkconfig(8)` man page contained an incorrect reference to runlevel 7, which does not exist (runlevels extend from 0 to 6, inclusive). This update corrects the man page by removing all references to "runlevel 7". ([BZ#466740](https://bugzilla.redhat.com/show_bug.cgi?id=466740)<sup>111</sup>)

\* the `ntsysv(8)` man page referenced a non-existent man page, `servicesconf`. This reference has been removed. ([BZ#516599](https://bugzilla.redhat.com/show_bug.cgi?id=516599)<sup>112</sup>)

All users of `chkconfig` are advised to upgrade to these updated packages, which resolve these issues.

## 1.19. cman

### 1.19.1. RHBA-2009:1435: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1435](https://errata.redhat.com/RHBA-2009:1435)<sup>113</sup>

Updated `cman` packages that fix a bug and add an enhancement are now available.

The Cluster Manager (`cman`) utility provides user-level services for managing a Linux cluster.

This update applies the following bug fix:

\* in several places internally, `cman` assumed a transition message meant the node in question (or the sending node) was joining the cluster rather than just sending its current post-transition state. In some circumstances, this could lead to `cman` killing the wrong nodes. With this update, `cman` now checks the `first_trans` flag, which is set when a node first encounters another node in the cluster. Only if `first_trans` is set does `cman` now consider the node as joining the cluster. ([BZ#518061](https://bugzilla.redhat.com/show_bug.cgi?id=518061)<sup>114</sup>)

Also, this update includes the following enhancement:

First, if a node was asked to remove a key (fence) for a device that it was not registered with, the node attempted to register with that device on-the-fly. With this update, when nodes are asked to remove a key from devices with which they are not registered, the fencing fails.

Second, for the common case of SAN environments with multiple Logical Unit Numbers (LUNs), the devices (LUNs) that can be unregistered must be ordered consistently on all nodes. Consistent ordering is not guaranteed by the Logical Volume Manager (LVM), however; device names can vary from node to node to prevent interleaving of fence operation among devices. With this update, the `fence_scsi` agent extracts the device name (`pv_name`) and Universally Unique Identifier (`pv_uuid`) and builds a hash keyed on the UUID (which is consistent on all nodes). This ensures devices are ordered consistently on each node.

---

<sup>110</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=501225](https://bugzilla.redhat.com/show_bug.cgi?id=501225)

<sup>111</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=466740](https://bugzilla.redhat.com/show_bug.cgi?id=466740)

<sup>112</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=516599](https://bugzilla.redhat.com/show_bug.cgi?id=516599)

<sup>114</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=518061](https://bugzilla.redhat.com/show_bug.cgi?id=518061)

Consequent to these two changes, the first node to fence removes the other node's key from the device or devices. The second node, now not registered with the device, is not able to fence the first. This allows fence\_scsi to work in a 2-node cluster. ([BZ#520823](#)<sup>115</sup>)

All cman users should install this updated package, which fixes this bug and enables users to use fence\_scsi in a 2-node environment.

### 1.19.2. RHBA-2009:1516: bug-fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1516](#)<sup>116</sup>

Updated cman packages that fix a bug are now available.

The Cluster Manager (cman) utility provides user-level services for managing a Linux cluster.

This update applies the following bug fix:

Add support for power cycle command to fence\_ipmi, which doesn't shut down the BMC controller.

Old behavior is still the default, so nothing changes without a configuration change. Now there is a new method option that can have the value "cycle", which uses the ipmi power cycle command.

Example of usage:...

```
<fencedevices> <fencedevice agent="fence_ipmilan_new" ipaddr="1.2.3.4" login="root"
name="ipmifd1" passwd="password" method="cycle" /> ...
```

Users are advised to upgrade to these updated cman packages, which resolve this issue.

### 1.19.3. RHBA-2009:1598: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1598](#)<sup>117</sup>

Updated cman packages that resolve several issues are now available.

[Updated 4 Jan 2009] This update provides improved descriptions of both bug fixes included in this advisory, and especially the description for bug 529712. The packages included in this revised update have not been changed in any way from those included in the original advisory.

The Cluster Manager (cman) utility provides user-level services for managing a Linux cluster.

These updated cman packages provide fixes for the following bugs:

\* when using device-mapper-multipath devices, registrations were only sent to the active path, which meant that, in the event of path failure, the node would be unable to access the device via the

<sup>115</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=520823](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=520823)



secondary path or paths because the device would not be registered with the secondary path(s). With this update, the presence of device-mapper-multipath devices is detected correctly, the right paths are discovered, and each path is registered, including secondary paths. ([BZ#529712](#)<sup>118</sup>)

\* when running the `/etc/init.d/scsi_reserve` init script to check for errors, such as an incorrect `cluster.conf` configuration, among others, upon finding an error the script did not print "[FAILED]" to standard output, as is convention for system services which encounter startup errors. With this update, the `scsi_reserve` init script has been fixed so that it prints "[FAILED]" to standard output when an error is encountered, and "[OK]" otherwise. Any errors encountered are logged to the system log. ([BZ#530400](#)<sup>119</sup>)

All users of `cman` are advised to upgrade to these updated packages, which resolve these issues.

### 1.19.4. RHBA-2009:1622: bug-fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1622](#)<sup>120</sup>

Updated `cman` packages that fix bugs are now available.

The Cluster Manager (`cman`) utility provides user-level services for managing a Linux cluster.

This update fixes the following bugs:

\* `qdiskd` erroneously writes the message "`qdiskd: read (system call) has hung for X seconds`". ([BZ 537157](#))

\* Crash in `fence_ipmilan` when `-M` switch was not present on the command-line. ([BZ 537157](#))

Users are advised to upgrade to these updated `cman` packages, which resolve these issues.

### 1.19.5. RHBA-2010:0266: bug fix and enhancement update

Updated `cman` packages that fix bugs and add enhancements are now available.

The Cluster Manager (`cman`) utility provides user-level services for managing a Linux cluster.

Changes in this update:

\* `fence_rsa` fails to login with new RSA II firmware. ([BZ#549473](#)<sup>121</sup>)

\* `fence_virsh` reports vm status incorrectly. ([BZ#544664](#)<sup>122</sup>)

\* improve error messages from `ccsd` if there is a network problem. ([BZ#517399](#)<sup>123</sup>)

\* new fence agent for VMWare. ([BZ#548577](#)<sup>124</sup>)

Note: this is a Tech Preview only.

---

<sup>118</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=529712](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=529712)

<sup>119</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=530400](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=530400)

<sup>121</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=549473](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=549473)

<sup>122</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=544664](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=544664)

<sup>123</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=517399](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=517399)

<sup>124</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=548577](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=548577)



- \* fence agent for HP iLO2 MP. ([BZ#508722](#)<sup>125</sup>)
- \* fence agent for RSB ends with traceback. ([BZ#545054](#)<sup>126</sup>)
- \* security feature for SNMP based agent: apc\_snmp & ibmblade. ([BZ#532922](#)<sup>127</sup>)
- \* change default timeout values for various fence agents. ([BZ#549124](#)<sup>128</sup>)
- \* "Option -V" (show version) was not working in all fence agents. ([BZ#549113](#)<sup>129</sup>)
- \* automatically configure consensus based on token timeout. ([BZ#544482](#)<sup>130</sup>)
- \* add readconfig & dumpconfig to fence\_tool. ([BZ#514662](#)<sup>131</sup>)
- \* make groupd handle partition merges. ([BZ#546082](#)<sup>132</sup>)
- \* groupd: clean up leaving failed node. ([BZ#521817](#)<sup>133</sup>)
- \* scsi\_reserve should always echo after failure. ([BZ#514260](#)<sup>134</sup>)
- \* fence\_scsi\_test: add debug information. ([BZ#516763](#)<sup>135</sup>)
- \* fence\_scsi\_test should not allow -c & -s options together. ([BZ#528832](#)<sup>136</sup>)
- \* fix fence\_ipmilan read from uninitialized memory. ([BZ#532138](#)<sup>137</sup>)
- \* make qdiskd stop crying wolf. ([BZ#532773](#)<sup>138</sup>)
- \* fencing failed when used without telnet or ssh. ([BZ#512343](#)<sup>139</sup>)
- \* APC changed product name (MasterSwitch -> Switched Rack PDU). ([BZ#447481](#)<sup>140</sup>)
- \* fix invalid initialization introduced by retry-on option.
- \* broken device detection for DRAC3 ERA/O. ([BZ#489809](#)<sup>141</sup>)
- \* fix case sensitivities in action parameter. ([BZ#528938](#)<sup>142</sup>)
- \* fencing\_snmp failed on all operations & traceback fix. ([BZ#528916](#)<sup>143</sup>)
- \* accept unknown options from standard input. ([BZ#532920](#)<sup>144</sup>)

<sup>125</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=508722](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=508722)

<sup>126</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=545054](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=545054)

<sup>127</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=532922](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=532922)

<sup>128</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=549124](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=549124)

<sup>129</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=549113](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=549113)

<sup>130</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=544482](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=544482)

<sup>131</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=514662](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=514662)

<sup>132</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=546082](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=546082)

<sup>133</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=521817](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=521817)

<sup>134</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=514260](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=514260)

<sup>135</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=516763](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=516763)

<sup>136</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=528832](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=528832)

<sup>137</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=532138](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=532138)

<sup>138</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=532773](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=532773)

<sup>139</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=512343](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=512343)

<sup>140</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=447481](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=447481)

<sup>141</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=489809](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=489809)

<sup>142</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=528938](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=528938)

<sup>143</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=528916](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=528916)

<sup>144</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=532920](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=532920)

- \* fence\_apc unable to obtain plug status. ([BZ#532916](https://bugzilla.redhat.com/show_bug.cgi?id=532916)<sup>145</sup>)
- \* timeout options added. ([BZ#507514](https://bugzilla.redhat.com/show_bug.cgi?id=507514)<sup>146</sup>)
- \* better default timeout for bladecenter. ([BZ#526806](https://bugzilla.redhat.com/show_bug.cgi?id=526806)<sup>147</sup>)
- \* the LOGIN\_TIMEOUT value was too short for fence\_lpar & the SSH login timed out before the connection could be completed. ([BZ#546340](https://bugzilla.redhat.com/show_bug.cgi?id=546340)<sup>148</sup>)
- \* add missing-as-off option (missing blade/device is always OFF). ([BZ#248006](https://bugzilla.redhat.com/show_bug.cgi?id=248006)<sup>149</sup>)
- \* make qdiskd "master-wins" node work. ([BZ#372901](https://bugzilla.redhat.com/show_bug.cgi?id=372901)<sup>150</sup>)
- \* make qdisk self-fence system if write errors take longer than interval\*tko. ([BZ#511113](https://bugzilla.redhat.com/show_bug.cgi?id=511113)<sup>151</sup>)
- \* make service\_cman.lcrso executable, so RPM adds it to the debuginfo pkg. ([BZ#511346](https://bugzilla.redhat.com/show_bug.cgi?id=511346)<sup>152</sup>)
- \* don't check for xm command in cman init script: virsh is more appropriate. ([BZ#516111](https://bugzilla.redhat.com/show_bug.cgi?id=516111)<sup>153</sup>)
- \* allow re-registering of a quorum device. ([BZ#525270](https://bugzilla.redhat.com/show_bug.cgi?id=525270)<sup>154</sup>)
- \* fix fence\_scsi, multipath & persistent reservations. ([BZ#516625](https://bugzilla.redhat.com/show_bug.cgi?id=516625)<sup>155</sup>)
- \* cman\_tool leave remove reduces quorum when no services are connected. ([BZ#515446](https://bugzilla.redhat.com/show_bug.cgi?id=515446)<sup>156</sup>)
- \* fence\_sanbox2 unable to retrieve status. ([BZ#512947](https://bugzilla.redhat.com/show_bug.cgi?id=512947)<sup>157</sup>)
- \* gfs\_controld: GETLK should free unused resource. ([BZ#513285](https://bugzilla.redhat.com/show_bug.cgi?id=513285)<sup>158</sup>)
- \* allow IP addresses as node names. ([BZ#504158](https://bugzilla.redhat.com/show_bug.cgi?id=504158)<sup>159</sup>)
- \* fence\_scsi man page contains invalid option. ([BZ#515731](https://bugzilla.redhat.com/show_bug.cgi?id=515731)<sup>160</sup>)
- \* fence\_scsi support for 2 node clusters. ([BZ#516085](https://bugzilla.redhat.com/show_bug.cgi?id=516085)<sup>161</sup>)
- \* Support for power cycle in fence ipmi. ([BZ#482913](https://bugzilla.redhat.com/show_bug.cgi?id=482913)<sup>162</sup>)
- \* add option 'list devices' for fencing agents. ([BZ#519697](https://bugzilla.redhat.com/show_bug.cgi?id=519697)<sup>163</sup>)
- \* add support for switching IPv4/IPv6. ([BZ#520458](https://bugzilla.redhat.com/show_bug.cgi?id=520458)<sup>164</sup>)

---

<sup>145</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=532916](https://bugzilla.redhat.com/show_bug.cgi?id=532916)

<sup>146</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=507514](https://bugzilla.redhat.com/show_bug.cgi?id=507514)

<sup>147</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=526806](https://bugzilla.redhat.com/show_bug.cgi?id=526806)

<sup>148</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=546340](https://bugzilla.redhat.com/show_bug.cgi?id=546340)

<sup>149</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=248006](https://bugzilla.redhat.com/show_bug.cgi?id=248006)

<sup>150</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=372901](https://bugzilla.redhat.com/show_bug.cgi?id=372901)

<sup>151</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=511113](https://bugzilla.redhat.com/show_bug.cgi?id=511113)

<sup>152</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=511346](https://bugzilla.redhat.com/show_bug.cgi?id=511346)

<sup>153</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=516111](https://bugzilla.redhat.com/show_bug.cgi?id=516111)

<sup>154</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=525270](https://bugzilla.redhat.com/show_bug.cgi?id=525270)

<sup>155</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=516625](https://bugzilla.redhat.com/show_bug.cgi?id=516625)

<sup>156</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=515446](https://bugzilla.redhat.com/show_bug.cgi?id=515446)

<sup>157</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=512947](https://bugzilla.redhat.com/show_bug.cgi?id=512947)

<sup>158</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=513285](https://bugzilla.redhat.com/show_bug.cgi?id=513285)

<sup>159</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=504158](https://bugzilla.redhat.com/show_bug.cgi?id=504158)

<sup>160</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=515731](https://bugzilla.redhat.com/show_bug.cgi?id=515731)

<sup>161</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=516085](https://bugzilla.redhat.com/show_bug.cgi?id=516085)

<sup>162</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=482913](https://bugzilla.redhat.com/show_bug.cgi?id=482913)

<sup>163</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=519697](https://bugzilla.redhat.com/show_bug.cgi?id=519697)

<sup>164</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=520458](https://bugzilla.redhat.com/show_bug.cgi?id=520458)

\* fence agent ends with traceback if option is missing. ([BZ#508262](#)<sup>165</sup>)

\* command line options to override default ports for different services, such as SSH & Telnet (i.e. -u option) were added. ([BZ#506928](#)<sup>167,166</sup>)

Note: "-u" does not currently work with fence\_wti. Other agents honor the port override command line options properly, however. ([BZ#506928](#)<sup>169,168</sup>)

\* force stdout close for fencing agents. ([BZ#518622](#)<sup>170</sup>)

\* support for long options. ([BZ#519670](#)<sup>171</sup>)

\* fix a situation where cman could kill the wrong nodes. ([BZ#513260](#)<sup>172</sup>)

\* fix support for >100 gfs & gfs2 file systems. ([BZ#561892](#)<sup>173</sup>)

\* fix a problem where 'dm suspend' would hang a withdrawn GFS file system. ([BZ#570530](#)<sup>174</sup>)

\* fix a problem where fence\_snmp returned success when the operation failed. ([BZ#573834](#)<sup>175</sup>)

\* fencing support for the new iDRAC interface included with Dell PowerEdge R710 & R910 blade servers was added. ([BZ#496748](#)<sup>176</sup>)

All cman users should install this update which makes these changes.

## 1.20. cmirror

### 1.20.1. RHBA-2010:0307: bug fix update

Updated cmirror packages that fix various bugs are now available.

The cmirror package is necessary for LVM-based mirroring (RAID1) in a cluster environment.

This update addresses the following issues:

\* the cmirror init script was reporting false errors in some 'stop' instances. ([BZ#520915](#)<sup>177</sup>)

\* the cluster log daemon was unable to recover if the cluster was shutdown and restarted without also restarting the cluster log daemon. ([BZ#518665](#)<sup>178</sup>)

\* communication structure used between nodes was not in a mixed-architecture or upgrade friendly format. ([BZ#488102](#)<sup>179</sup>)

<sup>165</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=508262](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=508262)

<sup>167</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=506928](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=506928)

<sup>166</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=506928](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=506928)

<sup>169</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=506928](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=506928)

<sup>168</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=506928](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=506928)

<sup>170</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=518622](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=518622)

<sup>171</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=519670](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=519670)

<sup>172</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=513260](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=513260)

<sup>173</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=561892](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=561892)

<sup>174</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=570530](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=570530)

<sup>175</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=573834](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=573834)

<sup>176</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=496748](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=496748)

<sup>177</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=520915](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=520915)

<sup>178</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=518665](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=518665)

<sup>179</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=488102](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=488102)

\* certain failure scenarios during cluster mirror device creation could lead to future kernel panics. ([BZ#544253](https://bugzilla.redhat.com/show_bug.cgi?id=544253)<sup>180</sup>)

All cmirror users should install these updated packages which fix these bugs.

### 1.21. cmirror-kmod

#### 1.21.1. RHBA-2010:0309: bug fix update

Updated kmod-cmirror packages that fix two bugs are now available.

The kmod-cmirror package is necessary for LVM-based mirroring (RAID1) in a cluster environment.

This update addresses the following issues:

\* error processing logic failed to remove a list item before freeing the associated memory. ([BZ#544253](https://bugzilla.redhat.com/show_bug.cgi?id=544253)<sup>182181</sup>)

\* added version number to the kernel/daemon communication structure. ([BZ#544253](https://bugzilla.redhat.com/show_bug.cgi?id=544253)<sup>184183</sup>)

All kmod-mirror users should install these updated packages, which fix these bugs.

### 1.22. conga

#### 1.22.1. RHBA-2009:1623: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1623](https://errata.redhat.com/RHBA-2009:1623)<sup>185</sup>

Updated conga packages that fix a regression introduced between Red Hat Enterprise Linux 5.3 and Red Hat Enterprise Linux 5.4 are now available.

The Conga project is a management system for remote workstations. It consists of luci, a secure web-based front-end, and ricci, a secure daemon that dispatches incoming messages to the underlying management modules.

This update applies the following bug fix:

\* the behavior of the virsh command changed between Red Hat Enterprise Linux 5.3 and Red Hat Enterprise Linux 5.4. In Red Hat Enterprise Linux 5.4, non-root users must add a "--read-only" flag to virsh commands for them to work correctly. The ricci component of conga runs the "virsh nodeinfo" command to determine whether a node can host a Virtual Machine service and it does so as a non-root user.

---

<sup>180</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=544253](https://bugzilla.redhat.com/show_bug.cgi?id=544253)

<sup>182</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=544253](https://bugzilla.redhat.com/show_bug.cgi?id=544253)

<sup>181</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=544253](https://bugzilla.redhat.com/show_bug.cgi?id=544253)

<sup>184</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=544253](https://bugzilla.redhat.com/show_bug.cgi?id=544253)

<sup>183</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=544253](https://bugzilla.redhat.com/show_bug.cgi?id=544253)

As a consequence, when run under Red Hat Enterprise Linux 5.4, running this command returned no information and the luci front-end did not provide an "Add a virtual machine service" option to Services in the Cluster tab for clusters that were expected to offer such services. With this update, ricci now runs a "virsh nodeinfo --readonly" command, in line with the changed behavior, and the web-based front end will provide options to add virtual machine services as expected. ([BZ#537209](https://bugzilla.redhat.com/show_bug.cgi?id=537209)<sup>186</sup>)

All conga users are advised to upgrade to these updated packages, which resolve this issue.

### 1.22.2. RHBA-2010:0289: bug fix and enhancement update

Updated Conga packages that fix numerous bugs (including a regression introduced between Red Hat Enterprise Linux 5.3 and Red Hat Enterprise Linux 5.4) and add the ability to reset user passwords when logged in to luci as an administrator are now available.

The Conga project is a management system for remote workstations. It consists of luci, which is a secure web-based front-end, and ricci, which is a secure daemon that dispatches incoming messages to underlying management modules.

This update applies the following bug fixes:

- \* The behavior of the virsh command changed between Red Hat Enterprise Linux 5.3 and Red Hat Enterprise Linux 5.4. In Red Hat Enterprise Linux 5.4, non-root users must add a "--read-only" flag to virsh commands. The ricci component runs the "virsh nodeinfo" command to determine whether a node can host a Virtual Machine service and it does so as a non-root user. As a consequence, when run under Red Hat Enterprise Linux 5.4, the "virsh nodeinfo" command returned no information and luci did not provide an "Add a virtual machine service" option to Services in the Cluster tab for clusters that were expected to offer such services. With this update, ricci now runs a "virsh nodeinfo --readonly" command in line with the changed behavior, and luci provides options to add Virtual Machine services as expected. ([BZ#519252](https://bugzilla.redhat.com/show_bug.cgi?id=519252)<sup>187</sup>)
- \* luci failed to start. ([BZ#469881](https://bugzilla.redhat.com/show_bug.cgi?id=469881)<sup>188</sup>)
- \* Conga doesn't run with SELinux. ([BZ#476698](https://bugzilla.redhat.com/show_bug.cgi?id=476698)<sup>189</sup>)
- \* Conga does not add the name of the managed system when adding an "LPAR Fencing" fence device to a node. ([BZ#508142](https://bugzilla.redhat.com/show_bug.cgi?id=508142)<sup>190</sup>)
- \* fs resource will remount itself if any configuration changes are made to cluster.conf. ([BZ#514051](https://bugzilla.redhat.com/show_bug.cgi?id=514051)<sup>191</sup>)
- \* luci does not validate passwords and incorrect characters can be used. ([BZ#519050](https://bugzilla.redhat.com/show_bug.cgi?id=519050)<sup>192</sup>)
- \* previously, the shebang lines in luci's python executables pointed to "/usr/bin/env python" rather than explicitly referencing the version of Python installed on the system. This broke those executables in the case where a user was installing an alternative Python version. With this update, all shebang lines point explicitly to the system version at /usr/bin/python. ([BZ#521884](https://bugzilla.redhat.com/show_bug.cgi?id=521884)<sup>193</sup>)
- \* Conga does not properly handle HA LVM types. ([BZ#530129](https://bugzilla.redhat.com/show_bug.cgi?id=530129)<sup>194</sup>)

<sup>186</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=537209](https://bugzilla.redhat.com/show_bug.cgi?id=537209)

<sup>187</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=519252](https://bugzilla.redhat.com/show_bug.cgi?id=519252)

<sup>188</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=469881](https://bugzilla.redhat.com/show_bug.cgi?id=469881)

<sup>189</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=476698](https://bugzilla.redhat.com/show_bug.cgi?id=476698)

<sup>190</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=508142](https://bugzilla.redhat.com/show_bug.cgi?id=508142)

<sup>191</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=514051](https://bugzilla.redhat.com/show_bug.cgi?id=514051)

<sup>192</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=519050](https://bugzilla.redhat.com/show_bug.cgi?id=519050)

<sup>193</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=521884](https://bugzilla.redhat.com/show_bug.cgi?id=521884)

<sup>194</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=530129](https://bugzilla.redhat.com/show_bug.cgi?id=530129)

This update adds the following enhancement:

- \* the ability to reset user passwords when logged in to luci as an administrator was added. ([BZ#519268](https://bugzilla.redhat.com/show_bug.cgi?id=519268)<sup>195</sup>)

All Conga users are advised to upgrade to these updated packages, which resolve these issues and add this enhancement.

## 1.23. coolkey

### 1.23.1. RHBA-2010:0068: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTRACK errata [RHBA-2010:0068](https://errata.redhat.com/RHBA-2010:0068)<sup>196</sup>

Updated coolkey packages that resolve several issues are now available.

The coolkey packages contain driver support for CoolKey and Common Access Card (CAC) smart card products.

These updated coolkey packages provide fixes for the following bugs:

- \* the Department of Defense's alternative CAC tokens are now supported by CoolKey. ([BZ#226790](https://bugzilla.redhat.com/show_bug.cgi?id=226790)<sup>197</sup>)
- \* the libcoolkeypk11.so shared object library, when it was not linked with the pthreads library, became unresponsive when the C\_Initialize() function was called following a call to syslog(). This update ensures that libcoolkeypk11.so does not hang when it is not linked with the pthreads threading library and the aforementioned scenario occurs. ([BZ#245529](https://bugzilla.redhat.com/show_bug.cgi?id=245529)<sup>199</sup><sup>198</sup>)
- \* CoolKey's PKCS#11 module failed to initialize when the C\_Initialize() function was called and the CKF\_OS\_LOCKING flag was set. This issue is related to the fix for [BZ#245529](https://bugzilla.redhat.com/show_bug.cgi?id=245529)<sup>201</sup><sup>200</sup>. With this update, the PKCS#11 module successfully initializes. ([BZ#443127](https://bugzilla.redhat.com/show_bug.cgi?id=443127)<sup>202</sup>)
- \* the Red Hat Enterprise Security Client (ESC) incorrectly identified CAC cards as CoolKey cards, and mistakenly opened the Phone Home dialog after doing so. With this update, CoolKey correctly identifies CAC cards and assigns the correct functionality to them.

With this fix, it is still possible to view certificates and diagnostics for CAC cards, though the management functions are now disabled. Finally, note that the RHBA-2010:0066 esc update must be installed in order to fully resolve this issue. ([BZ#499976](https://bugzilla.redhat.com/show_bug.cgi?id=499976)<sup>203</sup>)

- \* CoolKeys is now able to recognize smart cards that use the T1 protocol, such as the SafeNet 330J, in addition to the T0-protocol cards supported previously. ([BZ#514298](https://bugzilla.redhat.com/show_bug.cgi?id=514298)<sup>204</sup>)

---

<sup>195</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=519268](https://bugzilla.redhat.com/show_bug.cgi?id=519268)

<sup>197</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=226790](https://bugzilla.redhat.com/show_bug.cgi?id=226790)

<sup>199</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=245529](https://bugzilla.redhat.com/show_bug.cgi?id=245529)

<sup>198</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=245529](https://bugzilla.redhat.com/show_bug.cgi?id=245529)

<sup>201</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=245529](https://bugzilla.redhat.com/show_bug.cgi?id=245529)

<sup>200</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=245529](https://bugzilla.redhat.com/show_bug.cgi?id=245529)

<sup>202</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=443127](https://bugzilla.redhat.com/show_bug.cgi?id=443127)

<sup>203</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=499976](https://bugzilla.redhat.com/show_bug.cgi?id=499976)

<sup>204</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=514298](https://bugzilla.redhat.com/show_bug.cgi?id=514298)

\* CoolKey now correctly handles cryptographic operations such as digital signing when using cards with 2048-bit keys. Previously, only 1024-bit keys were supported. ([BZ#514299](#)<sup>205</sup>)

All users of coolkey are advised to upgrade to these updated packages, which resolve these issues.

## 1.24. coreutils

### 1.24.1. RHBA-2009:1511: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1511](#)<sup>206</sup>

An updated coreutils package that fixes a regression in the df command is now available.

The coreutils package contains core GNU utilities. It is a combination of the old GNU fileutils, sh-utils, and textutils packages.

This update fixes the following bug:

\* the coreutils update included with Red Hat Enterprise Linux 5.4 introduced a regression in the df command. Running "df -l" with a specific device specified (for example, "df -l /dev/hda1") resulted in a "Permission denied" message for regular users. This update corrects the regression: specifying a device now works for regular users as it did previously. Note: running "df -l" to list all devices was not affected by this bug: it worked as expected previously and continues to do so subsequent to this update. ([BZ#528641](#)<sup>207</sup>)

All coreutils users should upgrade to this updated package, which addresses this regression.

### 1.24.2. RHBA-2010:0120: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2010:0120](#)<sup>208</sup>

An updated coreutils package that fixes a bug in the readlink command is now available.

The coreutils package contains core GNU utilities. It is a combination of the old GNU fileutils, sh-utils, and textutils packages.

This update fixes the following bug:

\* when a directory contained a symbolic link to itself, the readlink command, which displays the value of a symbolic link on standard output, incorrectly gave the following error message when attempting to read the value of the symbolic link (or the value of the symbolic links when recursing through the

<sup>205</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=514299](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=514299)

<sup>207</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=528641](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=528641)



directory and its symlink): "Too many levels of symbolic links". With this update, readlink is once again able to correctly resolve and output the value of the recursive symbolic links to containing directories, or "directory loops", thus resolving the issue. ([BZ#567545](#)<sup>209</sup>)

All coreutils users should upgrade to this updated package, which addresses this regression.

## 1.25. cpio

### 1.25.1. RHSA-2010:0144: Moderate security update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2010:0144](#)<sup>210</sup>

An updated cpio package that fixes two security issues is now available for Red Hat Enterprise Linux 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

GNU cpio copies files into or out of a cpio or tar archive.

A heap-based buffer overflow flaw was found in the way cpio expanded archive files. If a user were tricked into expanding a specially-crafted archive, it could cause the cpio executable to crash or execute arbitrary code with the privileges of the user running cpio. ([CVE-2010-0624](#)<sup>211</sup>)

Red Hat would like to thank Jakob Lell for responsibly reporting the [CVE-2010-0624](#)<sup>212</sup> issue.

A denial of service flaw was found in the way cpio expanded archive files. If a user expanded a specially-crafted archive, it could cause the cpio executable to crash. ([CVE-2007-4476](#)<sup>213</sup>)

Users of cpio are advised to upgrade to this updated package, which contains backported patches to correct these issues.

## 1.26. cpuspeed

### 1.26.1. RHBA-2010:0035: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2010:0035](#)<sup>214</sup>

---

<sup>209</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=567545](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=567545)

<sup>211</sup> <https://www.redhat.com/security/data/cve/CVE-2010-0624.html>

<sup>212</sup> <https://www.redhat.com/security/data/cve/CVE-2010-0624.html>

<sup>213</sup> <https://www.redhat.com/security/data/cve/CVE-2007-4476.html>



An updated cpuspeed package that fixes some initscript exit statuses, avoids loading on problematic CPUs, and starts only after syslogd is now available.

The cpuspeed package configures CPU frequency scaling.

This update fixes the following bugs:

- \* some exit status codes from the initscript were not in line with LSB standards. The codes were updated, and are now compliant. ([BZ#495049](#)<sup>215</sup>)
- \* where Intel Xeon Processor 7100 series processors were used with Hyper-Threading Technology enabled, cpuspeed loading could create system deadlocks. The cpuspeed settings were changed and system deadlocks no longer occur on this hardware. ([BZ#449004](#)<sup>216</sup>)
- \* the cpuspeed initscript uses syslog to log important information about its status. However, cpuspeed was being started before syslog on boot, and log messages generated by the cpuspeed init script were not being captured. The cpuspeed init script now runs after the syslog init script, and all log messages are now being recorded. ([BZ#516224](#)<sup>217</sup>)

Users should upgrade to this updated package, which resolves these issues.

## 1.27. crash

### 1.27.1. RHBA-2010:0230: bug fix update

Updated crash packages that fix various bugs and add enhancements are now available.

The crash package is a core analysis suite. It is a self-contained tool that can be used to investigate either live systems, kernel core dumps created from the netdump, diskdump, and kdump packages from Red Hat Linux, the mcore kernel patch offered by Mission Critical Linux, or the LKCD kernel patch.

- \* if a kdump NMI was issued and the task kernel stack was changed, the backtrace would in some cases fail and produce an error: "bt: cannot transition from exception stack to current process stack". The crash package was updated to report task inconsistencies and change the active task as appropriate. Additionally, a new set -a option was added to manually set tasks to be the active task on its CPU. ([BZ#504952](#)<sup>218</sup>)
- \* if the kernel data structures in a non-matching vmlinux varied widely enough from the kernel that generated the vmcore, erroneous data could be read and consumed. Several new defensive mechanisms have been added and it now fails in a more reasonable manner. ([BZ#508156](#)<sup>219</sup>)
- \* running the bt -a command against a Xen hypervisor resulted in a "cannot resolve stack trace" warning message if the CPU received its shutdown NMI while running in an interrupt handler. The bt command was changed and the error no longer occurs. ([BZ#510505](#)<sup>220</sup>)
- \* added support for dumpfile format of virsh dump of KVM kernels. ([BZ#510519](#)<sup>221</sup>)

---

<sup>215</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=495049](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=495049)

<sup>216</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=449004](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=449004)

<sup>217</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=516224](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=516224)

<sup>218</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=504952](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=504952)

<sup>219</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=508156](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=508156)

<sup>220</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=510505](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=510505)

<sup>221</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=510519](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=510519)

\* if a dump was collected when there were one or more cpus offline in the system, an initialization-time failure would occur and the crash would abort. A patch was backported from upstream and the failure no longer occurs. ([BZ#520506](https://bugzilla.redhat.com/show_bug.cgi?id=520506)<sup>222</sup>)

\* running the 64-bit bt command could potentially start the backtrace of an active non-crashing task on its per-cpu IRQ stack, cause a faulty transition back to the process stack, the dumping of a bogus exception frame and the message "bt: WARNING: possibly bogus exception frame". The bt command was changed and it now starts from the NMI exception stack, the error no longer occurs. ([BZ#523512](https://bugzilla.redhat.com/show_bug.cgi?id=523512)<sup>223</sup>)

\* when the cpu\_possible\_map contains more CPUs than the cpu\_online\_map, the set, bt, runq and ps commands would reflect the existing but unused swapper tasks on the non-existent CPUs. The 64-bit PowerPC CPU count determination was fixed and the commands now run as expected. ([BZ#550419](https://bugzilla.redhat.com/show_bug.cgi?id=550419)<sup>224</sup>)

\* when INIT-generated pseudo-tasks were running in user-space and the kernel was unable to modify the kernel stack, the backtrace would not identify the interrupted task and would display a "bt: unwind: failed to locate return link" error message. The Itanium backtraces were fixed, and the backtrace now offers information regarding the task that was interrupted. The error message is also suppressed. (BZ #553353)

\* using dump to analyze very large xendump core files with ELF sections located beyond a file offset of 4GB resulted in errors. Changes were made to the xc\_core\_verify() initialization code and dump now works as expected. (BZ #561767)

\* The crash utility was rebased. See the changelog linked to in the references section below for full details. ([BZ#528184](https://bugzilla.redhat.com/show_bug.cgi?id=528184)<sup>225</sup>)

All users of crash are advised to upgrade to these updated packages, which resolve these issues.

## 1.28. ctdb

### 1.28.1. RHEA-2010:0320: enhancement update

The ctdb package is now available on the ClusterStorage channel.

CTDB is a clustered database based on Samba's Trivial Database (TDB). The ctdb package is a cluster implementation used to store temporary data. If an application is already using TBD for temporary data storage, it can be very easily converted to be cluster-aware and use CTDB.

This update makes the following change:

\* CTDB was previously available in the Supplementary channel and is now available in the ClusterStorage channel. ([BZ#558493](https://bugzilla.redhat.com/show_bug.cgi?id=558493)<sup>226</sup>)

Note that CTDB is included as a Technology Preview. Technology Preview features are included in Red Hat Enterprise Linux to provide the features with wide exposure, with the goal of supporting these features in a future release of Red Hat Enterprise Linux. Technology Preview features are not supported under Red Hat Enterprise Linux 5.5 subscription services, and may not be functionally

---

<sup>222</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=520506](https://bugzilla.redhat.com/show_bug.cgi?id=520506)

<sup>223</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=523512](https://bugzilla.redhat.com/show_bug.cgi?id=523512)

<sup>224</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=550419](https://bugzilla.redhat.com/show_bug.cgi?id=550419)

<sup>225</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=528184](https://bugzilla.redhat.com/show_bug.cgi?id=528184)

<sup>226</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=558493](https://bugzilla.redhat.com/show_bug.cgi?id=558493)

complete. Red Hat welcomes customer feedback and suggestions for Technology Previews. Advisories will be provided for high-severity security issues in Technology Preview features.

All users requiring CTDB should install these newly released packages, which add this enhancement.

## 1.29. cups

### 1.29.1. RHBA-2010:0045: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2010:0045](#)<sup>227</sup>

Updated cups packages that fix a severe memory leak in the CUPS scheduler are now available.

The Common UNIX Printing System (CUPS) provides a portable printing layer for UNIX and Unix-like operating systems.

This update addresses the following issue:

\* when adding or modifying many printer queues, cupsd, the CUPS scheduler leaked memory. For example, running "lpstat" after creating several thousand printer queues caused cupsd to use all available memory, eventually killing other processes and bringing the system down. With this update cupsd no longer leaks memory when adding or modifying large numbers of printer queues and the associated out-of-memory errors and crashes no longer occur. ([BZ#552213](#)<sup>228</sup>)

All cups users should upgrade to these updated packages, which resolves this issue.

### 1.29.2. RHSA-2010:0129: Moderate security update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2010:0129](#)<sup>229</sup>

Updated cups packages that fix one security issue are now available for Red Hat Enterprise Linux 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The Common UNIX Printing System (CUPS) provides a portable printing layer for UNIX operating systems.

It was discovered that the Red Hat Security Advisory RHSA-2009:1595 did not fully correct the use-after-free flaw in the way CUPS handled references in its file descriptors-handling interface. A remote attacker could send specially-crafted queries to the CUPS server, causing it to crash. ([CVE-2010-0302](#)<sup>230</sup>)

<sup>228</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=552213](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=552213)

<sup>230</sup> <https://www.redhat.com/security/data/cve/CVE-2010-0302.html>

Users of cups are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. After installing the update, the cupsd daemon will be restarted automatically.

### 1.29.3. RHSA-2009:1595: Moderate security update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2009:1595](#)<sup>231</sup>

Updated cups packages that fix multiple security issues are now available for Red Hat Enterprise Linux 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

[Updated 12th January 2010] The packages list in this erratum has been updated to include missing i386 packages for Red Hat Enterprise Linux Desktop and RHEL Desktop Workstation.

The Common UNIX Printing System (CUPS) provides a portable printing layer for UNIX operating systems.

A use-after-free flaw was found in the way CUPS handled references in its file descriptors-handling interface. A remote attacker could, in a specially-crafted way, query for the list of current print jobs for a specific printer, leading to a denial of service (cupsd crash). ([CVE-2009-3553](#)<sup>232</sup>)

Several cross-site scripting (XSS) flaws were found in the way the CUPS web server interface processed HTML form content. If a remote attacker could trick a local user who is logged into the CUPS web interface into visiting a specially-crafted HTML page, the attacker could retrieve and potentially modify confidential CUPS administration data. ([CVE-2009-2820](#)<sup>233</sup>)

Red Hat would like to thank Aaron Sigel of Apple Product Security for responsibly reporting the [CVE-2009-2820](#)<sup>234</sup> issue.

Users of cups are advised to upgrade to these updated packages, which contain backported patches to correct these issues. After installing the update, the cupsd daemon will be restarted automatically.

### 1.29.4. RHSA-2009:1513: Moderate security update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2009:1513](#)<sup>235</sup>

Updated cups packages that fix two security issues are now available for Red Hat Enterprise Linux 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

---

<sup>232</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3553.html>

<sup>233</sup> <https://www.redhat.com/security/data/cve/CVE-2009-2820.html>

<sup>234</sup> <https://www.redhat.com/security/data/cve/CVE-2009-2820.html>

The Common UNIX Printing System (CUPS) provides a portable printing layer for UNIX operating systems. The CUPS "pdftops" filter converts Portable Document Format (PDF) files to PostScript.

Two integer overflow flaws were found in the CUPS "pdftops" filter. An attacker could create a malicious PDF file that would cause "pdftops" to crash or, potentially, execute arbitrary code as the "lp" user if the file was printed. ([CVE-2009-3608](https://www.redhat.com/security/data/cve/CVE-2009-3608.html)<sup>236</sup>, [CVE-2009-3609](https://www.redhat.com/security/data/cve/CVE-2009-3609.html)<sup>237</sup>)

Red Hat would like to thank Chris Rohlf for reporting the [CVE-2009-3608](https://www.redhat.com/security/data/cve/CVE-2009-3608.html)<sup>238</sup> issue.

Users of cups are advised to upgrade to these updated packages, which contain a backported patch to correct these issues. After installing the update, the cupsd daemon will be restarted automatically.

## 1.29.5. RHBA-2010:0210: bug fix update

Updated cups packages that fix several bugs are now available.

The Common UNIX Printing System (CUPS) provides a portable printing layer for UNIX operating systems.

These updated packages address the following bugs:

- \* landscape orientation jobs had incorrect page margins. This affects all landscape orientation PDF files, including any landscape job printed from Mac OS X. ([BZ#447987](https://bugzilla.redhat.com/show_bug.cgi?id=447987)<sup>239</sup>)
- \* when running PHP files through the scheduler's web interface the wrong version PHP interpreter was used, causing missing header lines. ([BZ#460898](https://bugzilla.redhat.com/show_bug.cgi?id=460898)<sup>240</sup>)
- \* the tmpwatch package is needed by cups but there was no package dependency on it. ([BZ#487495](https://bugzilla.redhat.com/show_bug.cgi?id=487495)<sup>241</sup>)
- \* there was a memory leak in the scheduler's handling of "file:" device URIs. ([BZ#496008](https://bugzilla.redhat.com/show_bug.cgi?id=496008)<sup>242</sup>)
- \* setting quota limits using the lpadm command did not work correctly. ([BZ#496082](https://bugzilla.redhat.com/show_bug.cgi?id=496082)<sup>243</sup>)
- \* there were several issues with CGI handling in the scheduler, causing custom CGI scripts not to work as expected. ([BZ#497632](https://bugzilla.redhat.com/show_bug.cgi?id=497632)<sup>244</sup>, [BZ#506316](https://bugzilla.redhat.com/show_bug.cgi?id=506316)<sup>245</sup>)
- \* the dependencies between the various sub-packages were not made explicit in the package requirements. ([BZ#502205](https://bugzilla.redhat.com/show_bug.cgi?id=502205)<sup>246</sup>)
- \* jobs with multiple files could be removed from a disabled queue when it is re-enabled. ([BZ#506257](https://bugzilla.redhat.com/show_bug.cgi?id=506257)<sup>247</sup>)
- \* the cups-lpd daemon, for handling RFC 1179 clients, could fail under load due to incorrect temporary file handling. ([BZ#523152](https://bugzilla.redhat.com/show_bug.cgi?id=523152)<sup>248</sup>)

<sup>236</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3608.html>

<sup>237</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3609.html>

<sup>238</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3608.html>

<sup>239</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=447987](https://bugzilla.redhat.com/show_bug.cgi?id=447987)

<sup>240</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=460898](https://bugzilla.redhat.com/show_bug.cgi?id=460898)

<sup>241</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=487495](https://bugzilla.redhat.com/show_bug.cgi?id=487495)

<sup>242</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=496008](https://bugzilla.redhat.com/show_bug.cgi?id=496008)

<sup>243</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=496082](https://bugzilla.redhat.com/show_bug.cgi?id=496082)

<sup>244</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=497632](https://bugzilla.redhat.com/show_bug.cgi?id=497632)

<sup>245</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=506316](https://bugzilla.redhat.com/show_bug.cgi?id=506316)

<sup>246</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=502205](https://bugzilla.redhat.com/show_bug.cgi?id=502205)

<sup>247</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=506257](https://bugzilla.redhat.com/show_bug.cgi?id=506257)

<sup>248</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=523152](https://bugzilla.redhat.com/show_bug.cgi?id=523152)

\* the CUPS PDF input filter is no longer a separate PDF handling implementation, and instead uses the pdftops program from the poppler-utils package directly. ([BZ#527429](#)<sup>249</sup>)

\* adding or modifying many queues could cause the scheduler to leak large amounts of memory. ([BZ#540646](#)<sup>250</sup>)

All cups users should upgrade to these updated packages, which resolve these issues.

## 1.30. curl

### 1.30.1. RHSA-2010:0273: Moderate security, bug fix and enhancement update

Updated curl packages that fix one security issue, various bugs, and add enhancements are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

cURL is a tool for getting files from FTP, HTTP, Gopher, Telnet, and DICT servers, using any of the supported protocols. cURL is designed to work without user interaction or any kind of interactivity.

Wesley Miaw discovered that when deflate compression was used, libcurl could call the registered write callback function with data exceeding the documented limit. A malicious server could use this flaw to crash an application using libcurl or, potentially, execute arbitrary code. Note: This issue only affected applications using libcurl that rely on the documented data size limit, and that copy the data to the insufficiently sized buffer. ([CVE-2010-0734](#)<sup>251</sup>)

This update also fixes the following bugs:

\* when using curl to upload a file, if the connection was broken or reset by the server during the transfer, curl immediately started using 100% CPU and failed to acknowledge that the transfer had failed. With this update, curl displays an appropriate error message and exits when an upload fails mid-transfer due to a broken or reset connection. ([BZ#479967](#)<sup>252</sup>)

\* libcurl experienced a segmentation fault when attempting to reuse a connection after performing GSS-negotiate authentication, which in turn caused the curl program to crash. This update fixes this bug so that reused connections are able to be successfully established even after GSS-negotiate authentication has been performed. ([BZ#517199](#)<sup>253</sup>)

As well, this update adds the following enhancements:

\* curl now supports loading Certificate Revocation Lists (CRLs) from a Privacy Enhanced Mail (PEM) file. When curl attempts to access sites that have had their certificate revoked in a CRL, curl refuses access to those sites. ([BZ#532069](#)<sup>254</sup>)

---

<sup>249</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=527429](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=527429)

<sup>250</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=540646](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=540646)

<sup>251</sup> <https://www.redhat.com/security/data/cve/CVE-2010-0734.html>

<sup>252</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=479967](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=479967)

<sup>253</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=517199](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=517199)

<sup>254</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=532069](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=532069)

\* the curl(1) manual page has been updated to clarify that the "--socks4" and "--socks5" options do not work with the IPv6, FTPS, or LDAP protocols. ([BZ#473128](#)<sup>255</sup>)

\* the curl utility's program help, which is accessed by running "curl -h", has been updated with descriptions for the "--ftp-account" and "--ftp-alternative-to-user" options. ([BZ#517084](#)<sup>256</sup>)

Users of curl should upgrade to these updated packages, which contain backported patches to correct these issues and add these enhancements. All running applications using libcurl must be restarted for the update to take effect.

## 1.31. cyrus-imapd

### 1.31.1. RHSA-2009:1459: Important security update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2009:1459](#)<sup>257</sup>

Updated cyrus-imapd packages that fix several security issues are now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The cyrus-imapd packages contain a high-performance mail server with IMAP, POP3, NNTP, and Sieve support.

Multiple buffer overflow flaws were found in the Cyrus IMAP Sieve implementation. An authenticated user able to create Sieve mail filtering rules could use these flaws to execute arbitrary code with the privileges of the Cyrus IMAP server user. ([CVE-2009-2632](#)<sup>258</sup>, [CVE-2009-3235](#)<sup>259</sup>)

Users of cyrus-imapd are advised to upgrade to these updated packages, which contain backported patches to resolve these issues. After installing the update, cyrus-imapd will be restarted automatically.

## 1.32. cyrus-sasl

### 1.32.1. RHBA-2010:0151: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2010:0151](#)<sup>260</sup>

<sup>255</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=473128](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=473128)

<sup>256</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=517084](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=517084)

<sup>258</sup> <https://www.redhat.com/security/data/cve/CVE-2009-2632.html>

<sup>259</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3235.html>



Updated cyrus-sasl packages that resolve an issue are now available.

The cyrus-sasl packages contain the Cyrus implementation of SASL. SASL is the Simple Authentication and Security Layer, a method for adding authentication support to connection-based protocols.

These updated cyrus-sasl packages fix the following bug:

\* multithreaded programs which used the Cyrus SASL libraries could have become unresponsive after attempting to perform authentication routines. This was caused by a failure to release a mutex lock on a data structure in the Cyrus SASL code, which resulted in a race condition, thus causing the program using the library to hang. This race condition has been fixed so that it is thread-safe in this update. ([BZ#568084](https://bugzilla.redhat.com/show_bug.cgi?id=568084)<sup>261</sup>)

All users of cyrus-sasl are advised to upgrade to these updated packages, which resolve this issue.

### 1.33. dbus

#### 1.33.1. RHSA-2010:0018: Moderate security update



##### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2010:0018](https://www.redhat.com/security/data/cve/RHSA-2010:0018)<sup>262</sup>

Updated dbus packages that fix a security issue are now available for Red Hat Enterprise Linux 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

D-Bus is a system for sending messages between applications. It is used for the system-wide message bus service and as a per-user-login-session messaging facility.

It was discovered that the Red Hat Security Advisory RHSA-2009:0008 did not correctly fix the denial of service flaw in the system for sending messages between applications. A local user could use this flaw to send a message with a malformed signature to the bus, causing the bus (and, consequently, any process using libdbus to receive messages) to abort. ([CVE-2009-1189](https://www.redhat.com/security/data/cve/CVE-2009-1189)<sup>263</sup>)

Note: Users running any application providing services over the system message bus are advised to test this update carefully before deploying it in production environments.

All users are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. For the update to take effect, all running instances of dbus-daemon and all running applications using the libdbus library must be restarted, or the system rebooted.

#### 1.33.2. RHBA-2010:0236: bug fix update

Updated dbus packages that fix a multilib conflict that could cause installation failure on 64-bit architectures are now available.

---

<sup>261</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=568084](https://bugzilla.redhat.com/show_bug.cgi?id=568084)

<sup>263</sup> <https://www.redhat.com/security/data/cve/CVE-2009-1189.html>



D-Bus is a system for sending messages between applications. It is used for the system-wide message bus service, and as a per-user-login-session messaging facility.

\* the dbus api help files (installed to `/usr/share/devhelp/books/dbus/api/` by default) included with the dbus-devel sub-package were previously automatically generated for each architecture. These auto-generated files contain different timestamps and internal links and, consequently, caused file conflicts with multilib that could prevent dbus-devel installation on 64-bit architectures. With this update, a pre-generated set of help files, `dbus-1.1.2-pregen-doc-api-html.tar.bz2`, has been added to the rpm. This removes the multilib file conflicts and allows installation of the dbus-devel sub-package in all circumstances. ([BZ#471359](#)<sup>264</sup>)

All D-Bus users should install these updated packages which resolve this issue.

## 1.34. dbus-python

### 1.34.1. RHBA-2009:1559: bug fix available



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1559](#)<sup>265</sup>

Updated dbus-python packages that fix an issue with the puplet package updater are now available for Red hat Enterprise Linux 5.

The dbus-python package provides a Python binding to the D-Bus system message bus.

This updated dbus-python package fixes the following bug:

\* the puplet icon in the GNOME Notification Area displays notifications when updated packages are available. However, due to an error in the dbus-python bindings, when updates were available, puplet failed to display a notification. This update corrects the dbus-python bindings with the result that puplet is once again able to notify the user of available updates. ([BZ#532142](#)<sup>266</sup>)

All users are advised to upgrade to this updated package, which resolves this issue.

## 1.35. device-mapper

### 1.35.1. RHBA-2010:0296: bug fix and enhancement update

Updated device-mapper packages that include various bug fixes and enhancements are now available.

The device-mapper packages provide a library required by logical volume management utilities such as LVM2 and dmraid.

This update applies the following bug fixes([BZ#536814](#)<sup>267</sup>):

<sup>264</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=471359](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=471359)

<sup>266</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=532142](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=532142)

<sup>267</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=536814](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=536814)

- \* Fixes crash when hash keys compared are different lengths.
- \* Restores umask when device node creation fails.
- \* Does not fork daemon when dmeventd cannot be found.

This update adds the following enhancements:

- \* Adds splitname command which splits given device name into subsystem constituents.
- \* Adds y|--yes option to dmsetup for default 'yes' answer to prompts.
- \* Adds subsystem, vg\_name, lv\_name, lv\_layer fields to dmsetup reports.
- \* Adds crypt target handling to libdevmapper tree nodes.

All users of device-mapper should upgrade to these updated packages, which resolve these issues and include these enhancements.

## 1.36. device-mapper-multipath

### 1.36.1. RHBA-2009:1645: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1645](#)<sup>268</sup>

Updated device-mapper-multipath packages that fix two bugs are now available.

The device-mapper-multipath packages provide tools to manage multipath devices by giving the device-mapper multipath kernel module instructions on what to do, as well as by managing the creation and removal of partitions for device-mapper devices.

This update addresses the following bugs:

- \* the udev rules for device-mapper-multipath were causing device-mapper to occasionally create multipath devices without using the user specified uid, gid, or mode. They have been replaced with equivalent rules that do not cause this issue. ([BZ#537761](#)<sup>269</sup>)
- \* when LUNs were unmapped from LSI storage arrays, the multipath rdac path checker was not marking the paths as failed. This caused IO to the device to hang instead of fail. The rdac path checker now marks unmapped LUNs as failed. ([BZ#538463](#)<sup>270</sup>)

Users are advised to upgrade to these updated device-mapper-multipath packages, which resolve these issues.

### 1.36.2. RHBA-2010:0255: bug fix and enhancement update

Updated device-mapper-multipath packages that fix several bugs and add various enhancements are now available.

---

<sup>269</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=537761](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=537761)

<sup>270</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=538463](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=538463)

The device-mapper-multipath packages provide tools to manage multipath devices using the device-mapper multipath kernel module.

This update applies the following bug fixes:

- \* The kpartx utility creates device maps from partition tables. Device-mapper devices with minor numbers greater than 255 caused kpartx to use the UUID from the wrong device when trying to create partitions. If the device had pre-existing partitions, kpartx would fail to create the new partitions. With this update, kpartx is now able to handle device-mapper devices with minor numbers greater than 255. ([BZ#526550](https://bugzilla.redhat.com/show_bug.cgi?id=526550)<sup>271</sup>)
- \* The udev rules for device-mapper-multipath were causing device-mapper to occasionally create multipath devices without using the user specified uid, gid, or mode. They have been replaced with equivalent rules that do not cause this issue. ([BZ#518575](https://bugzilla.redhat.com/show_bug.cgi?id=518575)<sup>272</sup>)
- \* When LUNs were unmapped from LSI storage arrays, the multipath rdac path checker was not marking the paths as failed. This caused IO to the device to hang instead of fail. The rdac path checker now marks unmapped LUNs as failed. ([BZ#531744](https://bugzilla.redhat.com/show_bug.cgi?id=531744)<sup>273</sup>)
- \* The failover path grouping policy was not ordering the paths by priority, causing multipath to failover to the wrong path for devices with manual failback. The multipath paths are now correctly ordered with the failover path grouping policy. ([BZ#537977](https://bugzilla.redhat.com/show_bug.cgi?id=537977)<sup>274</sup>)
- \* On some storage devices, if a LUN is deleted from an existing multipath device, and a new LUN is presented to the host, it may end up with the same LUN ID and name as the old LUN. In this case, multipath will assume that this is the old LUN and belongs to the existing multipath device. This cause corruption. A new path checker "hp\_tur" has been added that verifies the WWID of the LUN when it checks the path, to avoid this problem. ([BZ#437585](https://bugzilla.redhat.com/show_bug.cgi?id=437585)<sup>275</sup>)
- \* The "tur" path checker was marking paths in standby mode as "failed". It now correctly marks them as "ghost". ([BZ#473039](https://bugzilla.redhat.com/show_bug.cgi?id=473039)<sup>276</sup>)
- \* Multipath wasn't correctly showing device renames in dry-run mode. This has been fixed. ([BZ#501019](https://bugzilla.redhat.com/show_bug.cgi?id=501019)<sup>277</sup>)
- \* Multipath was incorrectly setting the hardware handler for HP StorageWorks devices. This has been fixed. ([BZ#475967](https://bugzilla.redhat.com/show_bug.cgi?id=475967)<sup>278</sup>)
- \* On some storage devices, multipath would display incorrect path information the first time multipath listed the paths after recovery. This has been fixed. ([BZ#499080](https://bugzilla.redhat.com/show_bug.cgi?id=499080)<sup>279</sup>)
- \* If a path is removed while it is still part of a multipath device, it was taking multipath minutes to mark it as failed. This should now happen immediately at the end of the next path checking interval. ([BZ#527754](https://bugzilla.redhat.com/show_bug.cgi?id=527754)<sup>280</sup>)

---

<sup>271</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=526550](https://bugzilla.redhat.com/show_bug.cgi?id=526550)

<sup>272</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=518575](https://bugzilla.redhat.com/show_bug.cgi?id=518575)

<sup>273</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=531744](https://bugzilla.redhat.com/show_bug.cgi?id=531744)

<sup>274</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=537977](https://bugzilla.redhat.com/show_bug.cgi?id=537977)

<sup>275</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=437585](https://bugzilla.redhat.com/show_bug.cgi?id=437585)

<sup>276</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=473039](https://bugzilla.redhat.com/show_bug.cgi?id=473039)

<sup>277</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=501019](https://bugzilla.redhat.com/show_bug.cgi?id=501019)

<sup>278</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=475967](https://bugzilla.redhat.com/show_bug.cgi?id=475967)

<sup>279</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=499080](https://bugzilla.redhat.com/show_bug.cgi?id=499080)

<sup>280</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=527754](https://bugzilla.redhat.com/show_bug.cgi?id=527754)

- \* the multipathd daemon needs constant access to /var/lib and /var/run. However it was not allowing any devices mounted under /var to be removed. Now it only keeps open what it needs. ([BZ#532424](#)<sup>281</sup>)
- \* the multipath checker functions were not using the default scsi timeouts. Instead, each checker set its own timeout. Now all checker functions with explicit timeouts use the scsi timeout set in /sys/block/sd<x>/device/timeout by default. This can be changed by setting the "checker\_timeout" option in /etc/multipath.conf([BZ#553042](#)<sup>282</sup>)
- \* Multipathd was printing extraneous error messages. This has been fixed. ([BZ#472171](#)<sup>283</sup>, [BZ#502128](#)<sup>284</sup>, [BZ#524178](#)<sup>285</sup>)
- \* The multipath man page had some mistakes and missing information. This has been fixed. ([BZ#481239](#)<sup>286</sup>, [BZ#510331](#)<sup>287</sup>, [BZ#554830](#)<sup>288</sup>)
- \* A locking error could cause multipathd to deadlock if it failed to create a multipath device correctly. This has been fixed (BZ #537281)

This update adds the following enhancements:

- \* Default configurations were added for more IBM, HP, SUN, and DELL devices. ([BZ#504619](#)<sup>289</sup>, [BZ#512243](#)<sup>290</sup>, [BZ#515171](#)<sup>291</sup>, [BZ#517896](#)<sup>292</sup>, [BZ#540882](#)<sup>293</sup>, [BZ#545882](#)<sup>294</sup>)
- \* The kpartx utility now supports DASDs devices with more then 65520 cylinders. ([BZ#524009](#)<sup>295</sup>)

All users are advised to upgrade to these updated packages, which resolve these issues and add these enhancements.

## 1.37. dhcp

### 1.37.1. RHBA-2010:0042: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2010:0042](#)<sup>296</sup>

---

<sup>281</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=532424](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=532424)

<sup>282</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=553042](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=553042)

<sup>283</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=472171](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=472171)

<sup>284</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=502128](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=502128)

<sup>285</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=524178](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=524178)

<sup>286</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=481239](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=481239)

<sup>287</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=510331](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=510331)

<sup>288</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=554830](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=554830)

<sup>289</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=504619](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=504619)

<sup>290</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=512243](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=512243)

<sup>291</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=515171](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=515171)

<sup>292</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=517896](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=517896)

<sup>293</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=540882](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=540882)

<sup>294</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=545882](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=545882)

<sup>295</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=524009](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=524009)

A dhcp update that fixes one memory leak is now available.

The Dynamic Host Configuration Protocol (DHCP) is a protocol that allows individual devices on an IP network to get their own network configuration information, including an IP address, a subnet mask, and a broadcast address. The dhcp package provides a relay agent and ISC DHCP service required to enable and administer DHCP on a network.

This update applies the following updates:

- \* a memory leak in the load\_balance\_mine() function caused dhcpd, the dhcp server, to leak approximately 20-30 octets per DHCPDISCOVER packet when the server was configured for failover and failover was in a normal state. This particular leak has been closed with this update. ([BZ#552211](https://bugzilla.redhat.com/show_bug.cgi?id=552211)<sup>297</sup>)

Note: depending on the specific DHCP setup on a given system, other memory leaks may still present. Please file a separate bug if DHCP appears to leak memory after applying this update.

All dhcp users should to apply this update which closes this memory leak.

### 1.37.2. RHBA-2010:0223: bug fix update

A dhcp update that fixes bugs is now available.

DHCP (Dynamic Host Configuration Protocol) is a protocol which allows individual devices on an IP network to get their own network configuration information (IP address, subnetmask, broadcast address, etc.) from a DHCP server.

These updated packages address the following issues:

- \* When a system running a dhclient received a very short lease (e.g a few seconds), it would constantly have to request a renewal of its lease. The system would spend so much time running the dhclient-script every time it made a request that it would become almost unresponsive. A patch has been added to the code, setting the minimum lease time to 60 seconds. By preventing very short lease times, the server no longer becomes unresponsive from an overload of renewal requests. ([BZ#498658](https://bugzilla.redhat.com/show_bug.cgi?id=498658)<sup>298</sup>)

- \* When the \$localClockFudge variable was empty, the /sbin/dhclient-script added an empty line to the /etc/ntp.conf file when renewing the DHCP lease. This caused the diff command to fail when there was no meaningful difference between the old and new files, thus restarting the NTP daemon unnecessarily. This put useless noise in the log files that get picked up by logwatch. This update provides a slight code change that configures the NTP daemon differently. The /etc/ntp.conf file now only runs if there is a useful value in the \$localClockFudge variable. ([BZ#532136](https://bugzilla.redhat.com/show_bug.cgi?id=532136)<sup>299</sup>)

- \* A memory leak in the load\_balance\_mine() function caused 20-30 octets per DHCPDISCOVER packet to be leaked when failover was in use and was in its normal state. This caused the performance of the server to be significantly diminished. This update fixes the memory leak in the load\_balance\_mine() function, allowing the server to perform correctly. ([BZ#534117](https://bugzilla.redhat.com/show_bug.cgi?id=534117)<sup>300</sup>)

Note: depending on the specific DHCP setup on a given system, other memory leaks may still present. Please file a separate bug if DHCP appears to leak memory after applying this update.

<sup>297</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=552211](https://bugzilla.redhat.com/show_bug.cgi?id=552211)

<sup>298</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=498658](https://bugzilla.redhat.com/show_bug.cgi?id=498658)

<sup>299</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=532136](https://bugzilla.redhat.com/show_bug.cgi?id=532136)

<sup>300</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=534117](https://bugzilla.redhat.com/show_bug.cgi?id=534117)

\* A syntax error was discovered in the code of the initscript for the dhcrelay. In the process of restarting, the service would shutdown, but the initscript would fail when attempting to start the service again. A patch has been added, correcting the syntax error in the code. This correction now allows the service to restart correctly. ([BZ#555672](https://bugzilla.redhat.com/show_bug.cgi?id=555672)<sup>301</sup>)

Users are advised to upgrade to these updated dhcp packages which resolve these issues.

## 1.38. dhcpv6

### 1.38.1. RHBA-2010:0196: bug fix update

Updated dhcpv6 packages that resolve several issues are now available.

The dhcpv6 packages implement the Dynamic Host Configuration Protocol (DHCP) for Internet Protocol version 6 (IPv6) networks, in accordance with RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6). DHCP is a protocol that allows individual devices on an IP network to get their own network configuration information. It consists of: dhcp6c(8), the DHCPv6 client daemon; dhcp6s(8), the DHCPv6 server daemon; and dhcp6r(8), the DHCPv6 relay agent.

These updated packages fix the following bugs:

\* previously, the DHCPv6 client was not removing the address assigned to an individual interface after it disconnected. Consequently, the interface kept the same IPv6 address after reconnection. In these updated packages a new IPv6 address is assigned to an interface after disconnecting and reconnecting. ([BZ#466251](https://bugzilla.redhat.com/show_bug.cgi?id=466251)<sup>302</sup>)

\* DHCPv6 request packets created by the DHCPv6 client did not contain the "IA" sub-field, which should contain the address advertised by the server. Consequently the DHCPv6 client might have encountered issues trying to interact with other DHCPv6 servers. With this update, the DHCPv6 client now correctly inserts the "IA" field, resolving this issue. ([BZ#476974](https://bugzilla.redhat.com/show_bug.cgi?id=476974)<sup>303</sup>)

\* previously, when the DHCPv6 client received the response after sending a "Confirm" message, the client decided if it needed to apply Duplicate Address Detection (DAD) based on the type of the identity-association (IA) construct in the response. However, the reply from the DHCPv6 server does not always contain an IA in the reply message. Consequently, when running the DHCPv6 client for a second time, the client may have triggered a segmentation fault. In these updated packages, the DHCPv6 client now checks if the reply has an IA before deciding if DAD needs to be applied, resolving this issue. ([BZ#515644](https://bugzilla.redhat.com/show_bug.cgi?id=515644)<sup>304</sup>)

All users of dhcpv6 are advised to upgrade to these updated packages, which resolve this issue.

---

<sup>301</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=555672](https://bugzilla.redhat.com/show_bug.cgi?id=555672)

<sup>302</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=466251](https://bugzilla.redhat.com/show_bug.cgi?id=466251)

<sup>303</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=476974](https://bugzilla.redhat.com/show_bug.cgi?id=476974)

<sup>304</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=515644](https://bugzilla.redhat.com/show_bug.cgi?id=515644)

## 1.39. dmidecode

### 1.39.1. RHEA-2009:1456: enhancement update



#### Note

This update has already been released (prior to the GA of this release) as errata *RHEA-2009:1456*<sup>305</sup>

An updated dmidecode package that adds enhancements is now available.

The dmidecode package provides utilities for extracting x86 and ia64 hardware information from the system BIOS or EFI, depending on the SMBIOS/DMI standard. This information typically includes system manufacturer, model name, serial number, BIOS version, and asset tag.

It also often includes usage status for the CPU sockets, expansion slots (such as AGP, PCI, and ISA) and memory module slots, and a list of input and output ports (such as serial, parallel and USB).

This updated package applies the following enhancement:

\* the previous version of the dmidecode package was based on an upstream version (2.9), which lacked support for various new hardware items. This updated package includes version 2.10, which updates support for SMBIOS specification version 2.6 and improves DDR3 memory reporting. It adds support for LGA1366 socket devices, decoding PCI-E Gen 2 slot IDs, and for a variety of processors, including the Intel Core i7 and Dual-Core Celeron and Xeon Dual-, Quad- and Multi-Core 3xxx, 5xxx and 7xxx series processors. ([BZ#520123](https://bugzilla.redhat.com/show_bug.cgi?id=520123))<sup>306</sup>

Users of dmidecode are advised to upgrade to this updated package, which includes this enhanced support.

### 1.39.2. RHEA-2010:0303: enhancement update

An updated dmidecode package that provides enhancements is now available.

The dmidecode package provides utilities for extracting x86 and Intel Itanium hardware information from the system BIOS or EFI, depending on the SMBIOS/DMI standard. This information typically includes system manufacturer, model name, serial number, BIOS version, and asset tag.

It also often includes usage status for the CPU sockets, expansion slots (such as AGP, PCI, and ISA) and memory module slots, and a list of input and output ports (such as serial, parallel and USB).

This updated package applies the following enhancement:

\* the previous version of the dmidecode package was based on an upstream version (2.9), which lacked support for various new hardware items. This updated package provides version 2.10, which updates support for SMBIOS specification version 2.6 and improves DDR3 memory reporting. It adds support for LGA1366 socket devices, decoding PCI-E Gen 2 slot IDs, and for a variety of processors, including the Intel Core i7 and Dual-Core Celeron and Xeon Dual-, Quad- and Multi-Core 3xxx, 5xxx and 7xxx series processors. ([BZ#518562](https://bugzilla.redhat.com/show_bug.cgi?id=518562))<sup>307</sup>

<sup>306</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=520123](https://bugzilla.redhat.com/show_bug.cgi?id=520123)

<sup>307</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=518562](https://bugzilla.redhat.com/show_bug.cgi?id=518562)



Users of dmidecode are advised to upgrade to this updated package, which includes this enhanced support.

### 1.40. dmraid

#### 1.40.1. RHBA-2010:0286: bug fix update

Updated dmraid packages that fix several bugs are now available.

The dmraid packages contain the ATARAID/DDF1 activation tool. The tool supports RAID device discovery and RAID set activation, and displays properties for ATARAID/DDF1-formatted RAID sets on Linux kernels using the device-mapper utility.

These updated dmraid packages fix the following bugs:

- \* the dmraid-events package was installing the dmevent\_syslogpattern.txt file to the /etc/logwatch/scripts/services directory. The dmevent\_syslogpattern.txt file is used by the logwatch service to record event logs. SELinux does not allow write access to the /etc/logwatch/scripts/services directory, and as a result the logwatch service was prevented from updating the log file. The dmraid-events package has now been updated to install the log file at /var/cache/logwatch/dmeventd/syslogpattern.txt, and the log file is updated as expected. ([BZ#513402](https://bugzilla.redhat.com/show_bug.cgi?id=513402)<sup>308</sup>)

- \* after a hard disk drive rebuild has been completed using dmraid, the LED lights on each disk belonging to the rebuilt RAID volume should turn off. Previously, if the rebuild was initiated manually using the 'dmraid -R' command, the light on the spare disk would remain illuminated, incorrectly indicating that the disk was still being built. When rebuilding automatically with the libdmraid-events library, the light would not remain lit as expected. The dmraid packages have been updated to turn off the light correctly after a manual disk rebuild, and the drive light now correctly indicates the drive state. ([BZ#514497](https://bugzilla.redhat.com/show_bug.cgi?id=514497)<sup>309</sup>)

- \* dmraid binaries in the /sbin directory previously relied on libraries in the /usr directory. Since the /sbin directory typically only contains programs executed by the root user, reliance on libraries in the /usr directory could result in reference conflicts. The dmraid packages have been updated to no longer rely on the /usr directory, and library references are now improved. ([BZ#516852](https://bugzilla.redhat.com/show_bug.cgi?id=516852)<sup>310</sup>)

- \* the dmraid-events-logwatch tool would take ownership of directories that were already owned by the logwatch package. This included the following directories:

- \* /etc/logwatch/conf \* /etc/logwatch/conf/services \* /etc/logwatch/scripts \* /etc/logwatch/scripts/services

As a consequence, the dmraid-events-logwatch tool and the logwatch package would conflict. The dmraid-events-logwatch package has been updated to own only /etc/logwatch/scripts/services/dmeventd directory, and the conflict no longer arises with the logwatch package. ([BZ#545876](https://bugzilla.redhat.com/show_bug.cgi?id=545876)<sup>311</sup>)

- \* modifications to Intel support in the libdmraid tool caused the SONAME field to change. This caused compatibility issues in python-pyblock symbolic links. The version number in the libdmraid tool's file name has been updated, which caused the dependencies to be automatically re-generated during

---

<sup>308</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=513402](https://bugzilla.redhat.com/show_bug.cgi?id=513402)

<sup>309</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=514497](https://bugzilla.redhat.com/show_bug.cgi?id=514497)

<sup>310</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=516852](https://bugzilla.redhat.com/show_bug.cgi?id=516852)

<sup>311</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=545876](https://bugzilla.redhat.com/show_bug.cgi?id=545876)



the build process. The symbolic link is now repaired and there are no compatibility issues between libdmraid and python-pyblock. ([BZ#556254](#)<sup>312</sup>)

\* the pthread\_mutex\_trylock symbol was not being exported against the libpthread tool. As a consequence, the libdmraid-events-isw.so object would not be loaded during activation of a RAID5 volume library, reporting that pthread\_mutex\_trylock was an undefined symbol. Linking has now been added to the libpthread tool, and pthread\_mutex\_trylock is successfully referenced in the libdmraid-events-isw.so object. ([BZ#567922](#)<sup>313</sup>)

All dmraid users should upgrade to these updated packages, which resolve these issues.

## 1.41. dogtail

### 1.41.1. RHBA-2010:0009: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2010:0009](#)<sup>314</sup>

An updated dogtail package that fixes two bugs is now available.

Dogtail is an automation framework that uses accessibility technologies to communicate with desktop applications. Dogtail exposes desktop elements in a hierarchical interface. The dogtail package includes the GUI tools Script Recorder (dogtail-recorder) and AT-SPI Browser (sniff). Script Recorder creates Python scripts based on user actions and AT-SPI Browser is a graphical browser of the desktop elements hierarchy exposed by Dogtail.

This updated dogtail package fixes the following bugs:

\* the destroyAbout function was undefined in the previous Dogtail release. Consequently, the Close button in the AT-SPI Browser About window (Help > About) did not work. This function is now properly defined; the showAbout function calls this function when the Close button is clicked; and the About window closes. Note: the close box in the title bar of the About window worked in both the earlier and current release. ([BZ#250219](#)<sup>315</sup>)

\* previously, the shebang lines in Dogtail's python scripts pointed to "/usr/bin/env python" rather than explicitly referencing the system-installed Python. This broke these scripts in the case of a user installing an alternative version of Python. With this update, all Dogtail's python scripts point explicitly to the system version at /usr/bin/python. ([BZ#521339](#)<sup>316</sup>)

All dogtail users should upgrade to this updated package, which resolves these issues.

<sup>312</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=556254](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=556254)

<sup>313</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=567922](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=567922)

<sup>315</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=250219](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=250219)

<sup>316</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=521339](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=521339)

### 1.42. dosfstools

#### 1.42.1. RHBA-2010:0007: bug fix update



##### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2010:0007](#)<sup>317</sup>

An updated dosfstools package that fixes two bugs is now available.

The dosfstools package includes the mkdosfs and dosfsck utilities, which respectively make and check File Allocation Table (FAT) file systems on hard drives or on floppies.

This updated package provides fixes for the following bugs:

\* when a FAT file system was created on a device-mapper device, if the drive geometry was not reported correctly to mkdosfs, the command printed it was "unable to get drive geometry" and was using the default drive geometry (255/63) instead. Because of an error, it did not, in fact, do this. Consequently, dosflabel could not set a label for the newly-created file system. With this update, the error in the mkdosfs command was corrected: when the drive geometry is not correctly reported, mkdosfs now sets the drive geometry to the default values as per its message to STD OUT. Consequently, FAT file systems created with mkdosfs are now correct and dosflabel can set its label. ([BZ#249067](#)<sup>318</sup>)

\* although dosfstools contains ELF objects, the dosfstools-debuginfo package was empty. With this update the -debuginfo package contains valid debugging information as expected. ([BZ#469842](#)<sup>319</sup>)

All dosfstools users should upgrade to this updated package, which resolves these issues.

### 1.43. dstat

#### 1.43.1. RHSA-2009:1619: Moderate security update



##### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2009:1619](#)<sup>320</sup>

An updated dstat package that fixes one security issue is now available for Red Hat Enterprise Linux 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

---

<sup>318</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=249067](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=249067)

<sup>319</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=469842](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=469842)

Dstat is a versatile replacement for the vmstat, iostat, and netstat tools. Dstat can be used for performance tuning tests, benchmarks, and troubleshooting.

Robert Buchholz of the Gentoo Security Team reported a flaw in the Python module search path used in dstat. If a local attacker could trick a local user into running dstat from a directory containing a Python script that is named like an importable module, they could execute arbitrary code with the privileges of the user running dstat. ([CVE-2009-3894](#)<sup>321</sup>)

All dstat users should upgrade to this updated package, which contains a backported patch to correct this issue.

## 1.44. e4fsprogs

### 1.44.1. RHBA-2010:0239: bug fix and enhancement update

Enhanced e4fsprogs packages that fix a bug are now available.

The e4fsprogs packages contain a number of utilities for creating, checking, modifying, and correcting inconsistencies in fourth extended (ext4 and ext4dev) file systems. e4fsprogs contains e4fsck (used to repair file system inconsistencies after an unclean shutdown), mke4fs (used to initialize a partition to contain an empty ext4 file system), tune4fs (used to modify file system parameters), and most other core ext4fs file system utilities.

The e4fsprogs packages have been upgraded to upstream version 1.41.9 for Red Hat Enterprise Linux 5.5. These updated packages contain several bug fixes over the previous version.

Important: These packages are now designed and intended to be installed alongside the original e2fsprogs package in Red Hat Enterprise Linux. As such, certain binaries in the e4fsprogs packages have been given new names. For example, the utility that checks ext4 file systems for consistency has been renamed to "e4fsck", thus allowing the original "e2fsck" program from the e2fsprogs package to coexist on the same system.

These updated e4fsprogs packages also include a fix for the following bug:

\* pygrub did not understand fourth extended (ext4) /boot partitions, and so was unable to paravirtualize guest domains. e4fsprogs-devel and ev4sprogs-libs packages are provided with this update for pygrub and other applications that require the new ext4 capable e2fsprogs libraries. ([BZ#528055](#)<sup>322</sup>)

All users of e4fsprogs are advised to upgrade to these updated packages, which resolve this issue.

## 1.45. elilo

### 1.45.1. RHEA-2010:0302: enhancement update

An updated elilo package that adds validation checks and error messages to the boot manager is now available.

---

<sup>321</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3894.html>

<sup>322</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=528055](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=528055)

ELILO is a Linux boot loader for Extensible Firmware Interface (EFI)-based systems, such as those running an Itanium CPU. [RHSAs-2009:1341](#)

This update add the following enhancement:

\* previously ELILO's boot manager, `efibootmgr`, returned only two error codes: "0" for success and "1" for failure. There are multiple reasons for the boot manager to fail, however, and diagnosing such failures was difficult with only one all-purpose error code. This update adds validation checks and error messages to identify boot manager failures depending upon the error condition encountered. Error messages now returned when `efibootmgr` fails include "partition is not valid"; "Failed to open extra arguments"; "Invalid hex characters in boot order" and others. ([BZ#250327](#)<sup>323</sup>)

All elilo users should upgrade to this updated package, which adds this feature.

## 1.46. elinks

### 1.46.1. [RHSAs-2009:1471](#): Important security update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSAs-2009:1471](#)<sup>324</sup>

An updated elinks package that fixes two security issues is now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

ELinks is a text-based Web browser. ELinks does not display any images, but it does support frames, tables, and most other HTML tags.

An off-by-one buffer overflow flaw was discovered in the way ELinks handled its internal cache of string representations for HTML special entities. A remote attacker could use this flaw to create a specially-crafted HTML file that would cause ELinks to crash or, possibly, execute arbitrary code when rendered. ([CVE-2008-7224](#)<sup>325</sup>)

It was discovered that ELinks tried to load translation files using relative paths. A local attacker able to trick a victim into running ELinks in a folder containing specially-crafted translation files could use this flaw to confuse the victim via incorrect translations, or cause ELinks to crash and possibly execute arbitrary code via embedded formatting sequences in translated messages. ([CVE-2007-2027](#)<sup>326</sup>)

All ELinks users are advised to upgrade to this updated package, which contains backported patches to resolve these issues.

---

<sup>323</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=250327](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=250327)

<sup>325</sup> <https://www.redhat.com/security/data/cve/CVE-2008-7224.html>

<sup>326</sup> <https://www.redhat.com/security/data/cve/CVE-2007-2027.html>

## 1.47. esc

### 1.47.1. RHBA-2010:0066: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2010:0066](#)<sup>327</sup>

An updated esc package that fixes various bugs is now available.

The esc package contains the Smart Card Manager tool, which allows users to manage security smart cards. The primary function of the tool is to enroll smart cards, so that they can be used for common cryptographic operations, such as secure email and website access.

This updated esc package includes fixes for the following bugs:

- \* The Enterprise Security Client incorrectly identified CAC cards as CoolKey cards and mistakenly opened the Phone Home connection dialog. With this update, CoolKey correctly identifies CAC cards and assigns the correct functionality to them. With this fix, it is still possible to view certificates and diagnostics for CAC cards, though the management functions are now disabled. RHBA-2010:9263, a CoolKey update, must also be installed to fully resolve this issue. ([BZ#467011](#)<sup>328</sup>)
- \* The Enterprise Security Client did not open the Phone Home connection dialog when a blank token was inserted. ([BZ#514053](#)<sup>329</sup>)
- \* Removing a smart card when the Enterprise Security Client was open could cause the Enterprise Security Client to terminate abnormally. With this update, removing smart cards should no longer cause the Enterprise Security Client to crash. ([BZ#517414](#)<sup>330</sup>)
- \* When creating a password for the Enterprise Security Client, using certain characters, such as the dollar sign and exclamation point, could cause a failure to enroll when entering the password later. This update fixes this problem so that using such symbols when creating passwords does not fail when attempting to enroll. ([BZ#549540](#)<sup>331</sup>)
- \* When the Enterprise Security Client was using an external user interface for enrollment and the UI page could not be downloaded because of a disconnected network or similar problem, then the user could neither enroll nor was made aware of the source of the problem. With this update, when such a situation occurs, a descriptive error message is sent to the user. ([BZ#549542](#)<sup>332</sup>)
- \* Inserting a CAC card into the computer causes the Enterprise Security Client to display an enabled "Enroll" button to the user erroneously because all management functions should be disabled for CAC cards. With this update, when a CAC card is entered, all management functions are disabled, including the "Enroll" function. ([BZ#553661](#)<sup>333</sup>)

<sup>328</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=467011](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=467011)

<sup>329</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=514053](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=514053)

<sup>330</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=517414](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=517414)

<sup>331</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=549540](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=549540)

<sup>332</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=549542](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=549542)

<sup>333</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=553661](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=553661)

All users of the Enterprise Security Client are advised to upgrade to this updated package, which resolves these issues.

### 1.48. etherboot

#### 1.48.1. RHBA-2010:0227: bug fix update

Updated etherboot packages that fix several bugs are now available.

Etherboot is a software package for creating ROM images (zrom files) that can download code over an Ethernet network to be executed on an x86 computer. Many network adapters have a socket where a ROM chip can be installed. Etherboot is code that can be put in such a ROM.

\* the zrom file for use with NE2000-compatible Ethernet cards used by etherboot when network booting using such a card failed to obtain an IP address. Consequently network booting a system with an NE2000-compatible Ethernet card failed, returning an error as follows:

```
Probing pci nic... Probing isa nic... [NE*000]
```

With this update the zrom file used by etherboot has been updated and network booting a KVM guest via PXE using NE2000 network card emulation now succeeds as expected. ([BZ#511912](https://bugzilla.redhat.com/show_bug.cgi?id=511912)<sup>334</sup>)

\* Change glibc32 BuildRequires to file-based BuildRequires. ([BZ#521901](https://bugzilla.redhat.com/show_bug.cgi?id=521901)<sup>335</sup>)

\* Use update-alternatives to provide the common /usr/share/qemu-pxe-roms directory. ([BZ#546016](https://bugzilla.redhat.com/show_bug.cgi?id=546016)<sup>336</sup>)

\* Use 0644 permission on all rom files. ([BZ#547773](https://bugzilla.redhat.com/show_bug.cgi?id=547773)<sup>337</sup>)

All etherboot users should install this update which addresses these issues.

### 1.49. ethtool

#### 1.49.1. RHBA-2010:0279: bug fix and enhancement update

An enhanced ethtool package that fixes a number of minor issues is now available.

The ethtool utility allows the querying and changing of specific settings on network adapters. These settings include speed, port, link auto-negotiation settings and PCI locations.

This updated package adds the following enhancements:

\* ethtool can now display all NIC speeds, not just 10/100/1000. ([BZ#450162](https://bugzilla.redhat.com/show_bug.cgi?id=450162)<sup>338</sup>)

\* the redundant INSTALL file has been removed from the package. ([BZ#472034](https://bugzilla.redhat.com/show_bug.cgi?id=472034)<sup>339</sup>)

---

<sup>334</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=511912](https://bugzilla.redhat.com/show_bug.cgi?id=511912)

<sup>335</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=521901](https://bugzilla.redhat.com/show_bug.cgi?id=521901)

<sup>336</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=546016](https://bugzilla.redhat.com/show_bug.cgi?id=546016)

<sup>337</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=547773](https://bugzilla.redhat.com/show_bug.cgi?id=547773)

<sup>338</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=450162](https://bugzilla.redhat.com/show_bug.cgi?id=450162)

<sup>339</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=472034](https://bugzilla.redhat.com/show_bug.cgi?id=472034)

\* the ethtool usage message has been fixed to not state that -h requires a DEVNAME. ([BZ#472038](#)<sup>340</sup>)

\* ethtool now recognizes 10000 as a valid speed and includes it as a supported link mode. ([BZ#524241](#)<sup>341</sup>, [BZ#529395](#)<sup>342</sup>)

All ethtool users should upgrade to this updated package which provides these enhancements.

## 1.50. evince

### 1.50.1. RHBA-2010:0195: bug fix update

An updated evince package that resolves various issues is now available.

evince is a GNOME-based document viewer.

This updated package resolves the following issues:

\* fullscreen mode allows a user to view (in a maximized window) just the document and a single navigation toolbar. Previously, the function that handles the timeout of fullscreen mode was only made aware of the window, rather than the workspace. Consequently, if a user switched to a different workspace while fullscreen mode was enabled, the fullscreen toolbar would persist the top of the screen. With this update, the evince fullscreen toolbar no longer remains after changing workspaces, resolving this issue. ([BZ#229173](#)<sup>343</sup>)

\* when searching for a string in a document, evince may have miscalculated the scope of the search if a string appeared more than once on a single page. Consequently, if a user was stepping through the search results using the "Find Next" button, evince would not step past the page with multiple matches. With this update, evince now correctly searches the whole document, resolving this issue. ([BZ#469379](#)<sup>344</sup>)

\* previously, evince classified a single error dialog as a full running instance. Consequently, if an instance of evince contained only an error dialog, any document opened would appear that instance. This may have confused users, as documents were displayed in the workspace where the error dialog is located, rather than the current workspace. In this updated package, evince no longer treats a single error dialog as an opened document, resolving this issue. ([BZ#504334](#)<sup>345</sup>)

\* when rendering a page of a PDF document, evince displays a blank page, with just the text "Loading..." visible until the page is ready to be viewed. Previously, evince was not checking if the drawing area for the loading page could be allocated. Consequently, if a PDF document with large page dimensions was opened evince may have crashed, returning a segmentation fault. With this update, the drawing area for the loading page is now correctly allocated, resolving this issue. ([BZ#499676](#)<sup>346</sup>)

All evince users are advised to upgrade to this updated package, which resolves these issues.

---

<sup>340</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=472038](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=472038)

<sup>341</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=524241](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=524241)

<sup>342</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=529395](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=529395)

<sup>343</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=229173](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=229173)

<sup>344</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=469379](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=469379)

<sup>345</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=504334](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=504334)

<sup>346</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=499676](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=499676)

### 1.51. exim

#### 1.51.1. RHBA-2009:1627: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2009:1627](#)<sup>347</sup>

Updated exim packages that resolve several issues are now available.

Exim is a message transfer agent (MTA) developed at the University of Cambridge for use on Unix systems connected to the Internet. It is freely available under the terms of the GNU General Public Licence. In style it is similar to Smail 3, but its facilities are more general. There is a great deal of flexibility in the way mail can be routed, and there are extensive facilities for checking incoming mail. Exim can be installed in place of sendmail, although the configuration of exim is quite different to that of sendmail.

These updated exim packages provide fixes for the following bugs:

- \* The exim init script would return with error code 0 regardless of if the service had actually been started. An incorrect return code would be issued concerning the exim init script because of an unimplemented feature of the script. These bugs concerning the exim init script have been corrected by modifying it to return a value of 2 on an unsupported command, a return of 1 when the `$NETWORKING` parameter is set to no, returning the correct status error to the user and forcing the script to restart (using `condrestart`) when the status is not equal to 0.
- \* The default configuration referred to an undefined domain list causing errors when trying to relay email. The correct domain list of `relay_to_domains` is now utilized.
- \* Exim listened on all interfaces by default, whereas Sendmail and Postfix only listen on loopback by default. Administrators who would assume exim had default settings configured the same as Sendmail and Postfix may have introduced a security hole when installing exim. To correct this the code segment `local_interfaces = <; 127.0.0.1 ; ::1;` has been added to the default configuration; allowing Administrators to treat exim default settings the same as Sendmail and Postfix.
- \* Exim used to attempt generation of the certificate on installation instead of the first start, which could cause the installation to fail when the certificate could not be generated. Certificate generation is now undertaken upon the first start of exim after installation, allowing the installation to succeed.

All users of exim are advised to upgrade to these updated packages, which resolve these issues.



## 1.52. fetchmail

### 1.52.1. RHSA-2009:1427: Moderate security update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2009:1427](#)<sup>348</sup>

An updated fetchmail package that fixes multiple security issues is now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

Fetchmail is a remote mail retrieval and forwarding utility intended for use over on-demand TCP/IP links, such as SLIP and PPP connections.

It was discovered that fetchmail is affected by the previously published "null prefix attack", caused by incorrect handling of NULL characters in X.509 certificates. If an attacker is able to get a carefully-crafted certificate signed by a trusted Certificate Authority, the attacker could use the certificate during a man-in-the-middle attack and potentially confuse fetchmail into accepting it by mistake. ([CVE-2009-2666](#)<sup>349</sup>)

A flaw was found in the way fetchmail handles rejections from a remote SMTP server when sending warning mail to the postmaster. If fetchmail sent a warning mail to the postmaster of an SMTP server and that SMTP server rejected it, fetchmail could crash. ([CVE-2007-4565](#)<sup>350</sup>)

A flaw was found in fetchmail. When fetchmail is run in double verbose mode ("-v -v"), it could crash upon receiving certain, malformed mail messages with long headers. A remote attacker could use this flaw to cause a denial of service if fetchmail was also running in daemon mode ("-d"). ([CVE-2008-2711](#)<sup>351</sup>)

Note: when using SSL-enabled services, it is recommended that the fetchmail "--sslcertck" option be used to enforce strict SSL certificate checking.

All fetchmail users should upgrade to this updated package, which contains backported patches to correct these issues. If fetchmail is running in daemon mode, it must be restarted for this update to take effect (use the "fetchmail --quit" command to stop the fetchmail process).

<sup>349</sup> <https://www.redhat.com/security/data/cve/CVE-2009-2666.html>

<sup>350</sup> <https://www.redhat.com/security/data/cve/CVE-2007-4565.html>

<sup>351</sup> <https://www.redhat.com/security/data/cve/CVE-2008-2711.html>

### 1.53. filesystem

#### 1.53.1. RHBA-2009:1481: bug fix update



##### Note

This update has already been released (prior to the GA of this release) as FASTRACK errata [RHBA-2009:1481](#)<sup>352</sup>

An updated filesystem package that corrects the owners of certain directories is now available for Red Hat Enterprise Linux 5.

The filesystem package is one of the basic packages that is installed on a Red Hat Linux system. Filesystem contains the basic directory layout for the Linux operating system, including the correct permissions for directories.

This updated filesystem package fixes the following bug:

\* a number of file system directories were unowned. This update corrects the ownership of the following directories: `/usr/src/debug`, `/usr/src/kernels`, several directories in `/usr/share/man`, `/usr/share/locale` and, under it, the `LC_MESSAGES` subdirectory for several locales. In addition, for the sake of consistency this updated filesystem package now owns, but does not create, the locale-specific man page directories located under `/usr/share/man/[locale]`. ([BZ#487568](#)<sup>353</sup>)

All users of filesystem are advised to upgrade to this updated package, which resolves this issue.

### 1.54. firefox

#### 1.54.1. RHSA-2010:0112: Critical security update



##### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2010:0112](#)<sup>354</sup>

Updated firefox packages that fix several security issues are now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having critical security impact by the Red Hat Security Response Team.

Mozilla Firefox is an open source Web browser. XULRunner provides the XUL Runtime environment for Mozilla Firefox.

A use-after-free flaw was found in Firefox. Under low memory conditions, visiting a web page containing malicious content could result in Firefox executing arbitrary code with the privileges of the user running Firefox. ([CVE-2009-1571](#)<sup>355</sup>)

---

<sup>353</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=487568](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=487568)

<sup>355</sup> <https://www.redhat.com/security/data/cve/CVE-2009-1571.html>

Several flaws were found in the processing of malformed web content. A web page containing malicious content could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox. ([CVE-2010-0159](#)<sup>356</sup>, [CVE-2010-0160](#)<sup>357</sup>)

Two flaws were found in the way certain content was processed. An attacker could use these flaws to create a malicious web page that could bypass the same-origin policy, or possibly run untrusted JavaScript. ([CVE-2009-3988](#)<sup>358</sup>, [CVE-2010-0162](#)<sup>359</sup>)

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 3.0.18. You can find a link to the Mozilla advisories in the References section of this errata.

All Firefox users should upgrade to these updated packages, which contain Firefox version 3.0.18, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

## 1.54.2. RHSA-2009:1674: Critical security update



### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2009:1674](#)<sup>360</sup>

Updated firefox packages that fix several security issues are now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having critical security impact by the Red Hat Security Response Team.

Mozilla Firefox is an open source Web browser. XULRunner provides the XUL Runtime environment for Mozilla Firefox.

Several flaws were found in the processing of malformed web content. A web page containing malicious content could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox. ([CVE-2009-3979](#)<sup>361</sup>, [CVE-2009-3981](#)<sup>362</sup>, [CVE-2009-3986](#)<sup>363</sup>)

A flaw was found in the Firefox NT Lan Manager (NTLM) authentication protocol implementation. If an attacker could trick a local user that has NTLM credentials into visiting a specially-crafted web page, they could send arbitrary requests, authenticated with the user's NTLM credentials, to other applications on the user's system. ([CVE-2009-3983](#)<sup>364</sup>)

A flaw was found in the way Firefox displayed the SSL location bar indicator. An attacker could create an unencrypted web page that appears to be encrypted, possibly tricking the user into believing they are visiting a secure page. ([CVE-2009-3984](#)<sup>365</sup>)

<sup>356</sup> <https://www.redhat.com/security/data/cve/CVE-2010-0159.html>

<sup>357</sup> <https://www.redhat.com/security/data/cve/CVE-2010-0160.html>

<sup>358</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3988.html>

<sup>359</sup> <https://www.redhat.com/security/data/cve/CVE-2010-0162.html>

<sup>361</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3979.html>

<sup>362</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3981.html>

<sup>363</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3986.html>

<sup>364</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3983.html>

<sup>365</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3984.html>

A flaw was found in the way Firefox displayed blank pages after a user navigates to an invalid address. If a user visits an attacker-controlled web page that results in a blank page, the attacker could inject content into that blank page, possibly tricking the user into believing they are viewing a legitimate page. ([CVE-2009-3985](https://www.redhat.com/security/data/cve/CVE-2009-3985)<sup>366</sup>)

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 3.0.16. You can find a link to the Mozilla advisories in the References section of this errata.

All Firefox users should upgrade to these updated packages, which contain Firefox version 3.0.16, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

### 1.54.3. RHSA-2009:1530: Critical security update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2009:1530](https://www.redhat.com/security/data/cve/RHSA-2009:1530)<sup>367</sup>

Updated Firefox packages that fix several security issues are now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having critical security impact by the Red Hat Security Response Team.

Mozilla Firefox is an open source Web browser. XULRunner provides the XUL Runtime environment for Mozilla Firefox. nspr provides the Netscape Portable Runtime (NSPR).

A flaw was found in the way Firefox handles form history. A malicious web page could steal saved form data by synthesizing input events, causing the browser to auto-fill form fields (which could then be read by an attacker). ([CVE-2009-3370](https://www.redhat.com/security/data/cve/CVE-2009-3370)<sup>368</sup>)

A flaw was found in the way Firefox creates temporary file names for downloaded files. If a local attacker knows the name of a file Firefox is going to download, they can replace the contents of that file with arbitrary contents. ([CVE-2009-3274](https://www.redhat.com/security/data/cve/CVE-2009-3274)<sup>369</sup>)

A flaw was found in the Firefox Proxy Auto-Configuration (PAC) file processor. If Firefox loads a malicious PAC file, it could crash Firefox or, potentially, execute arbitrary code with the privileges of the user running Firefox. ([CVE-2009-3372](https://www.redhat.com/security/data/cve/CVE-2009-3372)<sup>370</sup>)

A heap-based buffer overflow flaw was found in the Firefox GIF image processor. A malicious GIF image could crash Firefox or, potentially, execute arbitrary code with the privileges of the user running Firefox. ([CVE-2009-3373](https://www.redhat.com/security/data/cve/CVE-2009-3373)<sup>371</sup>)

A heap-based buffer overflow flaw was found in the Firefox string to floating point conversion routines. A web page containing malicious JavaScript could crash Firefox or, potentially, execute arbitrary code with the privileges of the user running Firefox. ([CVE-2009-1563](https://www.redhat.com/security/data/cve/CVE-2009-1563)<sup>372</sup>)

---

<sup>366</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3985.html>

<sup>368</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3370.html>

<sup>369</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3274.html>

<sup>370</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3372.html>

<sup>371</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3373.html>

<sup>372</sup> <https://www.redhat.com/security/data/cve/CVE-2009-1563.html>

A flaw was found in the way Firefox handles text selection. A malicious website may be able to read highlighted text in a different domain (e.g. another website the user is viewing), bypassing the same-origin policy. ([CVE-2009-3375](#)<sup>373</sup>)

A flaw was found in the way Firefox displays a right-to-left override character when downloading a file. In these cases, the name displayed in the title bar differs from the name displayed in the dialog body. An attacker could use this flaw to trick a user into downloading a file that has a file name or extension that differs from what the user expected. ([CVE-2009-3376](#)<sup>374</sup>)

Several flaws were found in the processing of malformed web content. A web page containing malicious content could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox. ([CVE-2009-3374](#)<sup>375</sup>, [CVE-2009-3380](#)<sup>376</sup>, [CVE-2009-3382](#)<sup>377</sup>)

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 3.0.15. You can find a link to the Mozilla advisories in the References section of this errata.

All Firefox users should upgrade to these updated packages, which contain Firefox version 3.0.15, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

### 1.54.4. RHSA-2009:1430: Critical security update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2009:1430](#)<sup>378</sup>

Updated firefox packages that fix several security issues are now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having critical security impact by the Red Hat Security Response Team.

Mozilla Firefox is an open source Web browser. XULRunner provides the XUL Runtime environment for Mozilla Firefox. nspr provides the Netscape Portable Runtime (NSPR).

Several flaws were found in the processing of malformed web content. A web page containing malicious content could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox. ([CVE-2009-3070](#)<sup>379</sup>, [CVE-2009-3071](#)<sup>380</sup>, [CVE-2009-3072](#)<sup>381</sup>, [CVE-2009-3074](#)<sup>382</sup>, [CVE-2009-3075](#)<sup>383</sup>)

A use-after-free flaw was found in Firefox. An attacker could use this flaw to crash Firefox or, potentially, execute arbitrary code with the privileges of the user running Firefox. ([CVE-2009-3077](#)<sup>384</sup>)

<sup>373</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3375.html>

<sup>374</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3376.html>

<sup>375</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3374.html>

<sup>376</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3380.html>

<sup>377</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3382.html>

<sup>379</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3070.html>

<sup>380</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3071.html>

<sup>381</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3072.html>

<sup>382</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3074.html>

<sup>383</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3075.html>

<sup>384</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3077.html>

A flaw was found in the way Firefox handles malformed JavaScript. A website with an object containing malicious JavaScript could execute that JavaScript with the privileges of the user running Firefox. ([CVE-2009-3079](https://www.redhat.com/security/data/cve/CVE-2009-3079.html)<sup>385</sup>)

Descriptions in the dialogs when adding and removing PKCS #11 modules were not informative. An attacker able to trick a user into installing a malicious PKCS #11 module could use this flaw to install their own Certificate Authority certificates on a user's machine, making it possible to trick the user into believing they are viewing a trusted site or, potentially, execute arbitrary code with the privileges of the user running Firefox. ([CVE-2009-3076](https://www.redhat.com/security/data/cve/CVE-2009-3076.html)<sup>386</sup>)

A flaw was found in the way Firefox displays the address bar when `window.open()` is called in a certain way. An attacker could use this flaw to conceal a malicious URL, possibly tricking a user into believing they are viewing a trusted site. ([CVE-2009-2654](https://www.redhat.com/security/data/cve/CVE-2009-2654.html)<sup>387</sup>)

A flaw was found in the way Firefox displays certain Unicode characters. An attacker could use this flaw to conceal a malicious URL, possibly tricking a user into believing they are viewing a trusted site. ([CVE-2009-3078](https://www.redhat.com/security/data/cve/CVE-2009-3078.html)<sup>388</sup>)

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 3.0.14. You can find a link to the Mozilla advisories in the References section of this errata.

All Firefox users should upgrade to these updated packages, which contain Firefox version 3.0.14, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

## 1.55. firstboot

### 1.55.1. RHBA-2010:0314: bug fix update

Updated firstboot packages that fix a bug are now available.

The firstboot utility runs after installation. It guides the user through a series of steps that allows for easier configuration of the machine.

These updated packages address the following issue:

\* Clicking [Change Network Configuration] from firstboot's network configuration page launched a separate network configuration window. If the user then clicked [Forward] on the still-visible main window, the separate configuration window became hidden behind the full-screen main window.

Further mouse-clicks would be ineffectual and it could appear to the user that the system had become unresponsive. It was necessary to use the alt+tab keys to reveal the hidden configuration window.

Code has been added to the `networking.py` source file to modify the behavior of the network configuration and main windows. Now the configuration window will stay on top if the user clicks outside its boundary. ([BZ#511984](https://bugzilla.redhat.com/show_bug.cgi?id=511984)<sup>389</sup>)

Users are advised to upgrade to these updated packages, which resolve this issue.

---

<sup>385</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3079.html>

<sup>386</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3076.html>

<sup>387</sup> <https://www.redhat.com/security/data/cve/CVE-2009-2654.html>

<sup>388</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3078.html>

<sup>389</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=511984](https://bugzilla.redhat.com/show_bug.cgi?id=511984)

## 1.56. freeradius

### 1.56.1. RHSA-2009:1451: Moderate security update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2009:1451](#)<sup>390</sup>

Updated freeradius packages that fix a security issue are now available for Red Hat Enterprise Linux 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

FreeRADIUS is a high-performance and highly configurable free Remote Authentication Dial In User Service (RADIUS) server, designed to allow centralized authentication and authorization for a network.

An input validation flaw was discovered in the way FreeRADIUS decoded specific RADIUS attributes from RADIUS packets. A remote attacker could use this flaw to crash the RADIUS daemon (radiusd) via a specially-crafted RADIUS packet. ([CVE-2009-3111](#)<sup>391</sup>)

Users of FreeRADIUS are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. After installing the update, radiusd will be restarted automatically.

### 1.56.2. RHBA-2009:1678: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTRACK errata [RHBA-2009:1678](#)<sup>392</sup>

Updated freeradius packages that fix a bug are now available.

FreeRADIUS is an Internet authentication daemon, which implements the RADIUS protocol, as defined in RFC 2865 (and others). It allows Network Access Servers (NAS boxes) to perform authentication for dial-up users. There are also RADIUS clients available for Web servers, firewalls, Unix logins, and more. Using RADIUS allows authentication and authorization for a network to be centralized, and minimizes the amount of re-configuration which has to be done when adding or deleting new users.

This update addresses the following bug:

\* an error in the EAP authentication module could cause memory corruption. Running the radeapclient utility would typically expose the problem. An error message including text such as this

```
*** glibc detected *** radeapclient: free(): invalid pointer:
```

<sup>391</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3111.html>

presented and `radeapclient` would then abort abnormally. This update corrects the error in the EAP authentication module. The module no longer corrupts memory and applications such as `radeapclient` that use this module work as expected. ([BZ#476513](#)<sup>393</sup>)

All `freeradius` users should install these updated packages, which fix this problem.

## 1.57. gail

### 1.57.1. RHBA-2009:1594: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTRACK errata [RHBA-2009:1594](#)<sup>394</sup>

Updated `gail` packages that resolve an issue are now available.

GAIL, the GNOME Accessibility Implementation Library, implements the abstract interfaces found in the Accessibility Toolkit (ATK) for GTK+ and GNOME libraries, and thereby enables accessibility technologies such as AT-SPI (the Assistive Technology Service Provider Interface) to access GUI elements.

These updated `gail` packages fix the following bug:

\* when starting a GNOME application at the shell prompt, the GAIL library incorrectly printed the following spurious error message when the "GNOME\_ACCESSIBILITY" environment variable was set to "0", which disables GNOME accessibility support: "GTK Accessibility Module initialized". With this update, this message no longer appears when the "GNOME\_ACCESSIBILITY" environment variable is set to "0". ([BZ#506561](#)<sup>395</sup>)

All users of `gail` are advised to upgrade to these updated packages, which resolve this issue.

## 1.58. gcc

### 1.58.1. RHBA-2009:1533: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1533](#)<sup>396</sup>

A `gcc` update that resolves an option handling bug where only the last "`-fno-builtin-*`" option specified on the command line was honored is now available.

The `gcc` packages include C, C++, Java, Fortran, Objective C, and Ada 95 GNU compilers, along with related support libraries.

---

<sup>393</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=476513](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=476513)

<sup>395</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=506561](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=506561)



This update fixes the following bug:

\* if multiple "-fno-builtin-\*" options were specified on the command line (for example, "-fno-builtin-iswalpha -fno-builtin-iswalnum") only the last option was honored (in the example, -fno-builtin-iswalnum). With this update, joined switches are no longer pruned, ensuring all such options are honored, as expected. ([BZ#526421](https://bugzilla.redhat.com/show_bug.cgi?id=526421)<sup>397</sup>)

Users are advised to install this gcc update, which applies this fix.

## 1.58.2. RHSA-2010:0039: Moderate and gcc4 security update



### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2010:0039](https://www.redhat.com/security/data/cve/RHSA-2010:0039)<sup>398</sup>

Updated gcc and gcc4 packages that fix one security issue are now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The gcc and gcc4 packages include, among others, C, C++, and Java GNU compilers and related support libraries. libgcj contains a copy of GNU Libtool's libltdl library.

A flaw was found in the way GNU Libtool's libltdl library looked for libraries to load. It was possible for libltdl to load a malicious library from the current working directory. In certain configurations, if a local attacker is able to trick a local user into running a Java application (which uses a function to load native libraries, such as System.loadLibrary) from within an attacker-controlled directory containing a malicious library or module, the attacker could possibly execute arbitrary code with the privileges of the user running the Java application. ([CVE-2009-3736](https://www.redhat.com/security/data/cve/CVE-2009-3736)<sup>399</sup>)

All gcc and gcc4 users should upgrade to these updated packages, which contain a backported patch to correct this issue. All running Java applications using libgcj must be restarted for this update to take effect.

## 1.58.3. RHBA-2010:0232: bug fix update

A gcc update that resolves several compiler bugs is now available.

The gcc packages include C, C++, Java, Fortran, Objective C, and Ada 95 GNU compilers, along with related support libraries.

This update applies the following bug fixes:

\* when compiling a debug version of a C++ program, it was possible for gcc to lose debug information for some local variables in C++ constructors or destructors. This was because gcc incorrectly released information on abstract functions (specifically, contents of the DECL\_INITIAL() function), which are needed for creating debug information. With this release, nodes containing abstract functions

<sup>397</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=526421](https://bugzilla.redhat.com/show_bug.cgi?id=526421)

<sup>399</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3736.html>

are flagged accordingly to prevent gcc from prematurely discarding needed debug information. ([BZ#513184](#)<sup>400</sup>)

\* when issuing multiple `-fno-builtin-*` switches to gcc, gcc only registered the last switch. With this release, gcc can now register multiple `-fno-builtin-*` switches correctly. ([BZ#515799](#)<sup>401</sup>)

\* in some cases, aggregates returned by value could cause reload failures in the caller function, resulting in an internal compiler error. This was caused by a bug in the combining code that incorrectly lengthens the lifetime of a hard register. This update applies a patch to `expand_call` function in `gcc/calls.c` that resolves the issue. ([BZ#516028](#)<sup>402</sup>)

\* using g++ to compile code containing virtual inheritances could result in a segmentation fault. This was because the `dynamic_cast` code in gcc did not use `src2dst` hints as expected; as a result, g++ could search an unnecessarily large address list for possible bases. With this release, the `dynamic_cast` code now uses `src2dst` hints; this allows g++ to defer searching bases that don't overlap with a virtual inheritance's address. ([BZ#519519](#)<sup>403</sup>)

\* On PowerPC, it was possible for DWARF access to function parameters to fail. This was caused by a bug in the GCC instruction set for PowerPC, where compiling with `-mno-sched-prolog` could discard debug location lists. This update fixes the bug, ensuring consistent DWARF access to function parameters on PowerPC. ([BZ#528792](#)<sup>404</sup>)

\* The libgcc unwinder now supports `DW_OP_swap` handling. This update also fixes bugs in the way unwinding code handled unwind information from `DW_OP_{gt,ge,lt,le}` and `DW_CFA_{remember,restore}_state`. ([BZ#555731](#)<sup>405</sup>)

All GCC users are advised to install this update.

## 1.59. gd

### 1.59.1. RHSA-2010:0003: Moderate security update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2010:0003](#)<sup>406</sup>

Updated gd packages that fix a security issue are now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The gd packages provide a graphics library used for the dynamic creation of images, such as PNG and JPEG.

---

<sup>400</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=513184](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=513184)

<sup>401</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=515799](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=515799)

<sup>402</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=516028](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=516028)

<sup>403</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=519519](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=519519)

<sup>404</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=528792](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=528792)

<sup>405</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=555731](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=555731)

A missing input sanitization flaw, leading to a buffer overflow, was discovered in the gd library. A specially-crafted GD image file could cause an application using the gd library to crash or, possibly, execute arbitrary code when opened. ([CVE-2009-3546](#)<sup>407</sup>)

Users of gd should upgrade to these updated packages, which contain a backported patch to resolve this issue.

## 1.60. gdb

### 1.60.1. RHBA-2010:0285: bug fix update

An updated gdb package that fixes various bugs is now available.

The GNU Project debugger, GDB, debugs programs written in C, C++, and other languages by executing them in a controlled fashion, and then printing out their data.

With this update, GDB is now re-based to upstream version 7.0.1 ([BZ#526533](#)<sup>408</sup>). This applies several bug fixes and enhancements not listed here. For a full description of this version, refer to the following link: <http://sourceware.org/cgi-bin/cvsweb.cgi/src/gdb/NEWS.diff?cvsroot=src&r1=t&tr1=1.259.2.1&r2=text&tr2=1.331.2.2&f=u>

This update applies the following bug fixes:

- \* Printing values from a debugged program by dereferencing a pointer to an object of dynamic type printed out an error stating "Cannot resolve DW\_OP\_push\_object\_address for a missing object". Such pointers are produced by an unsupported iFort compiler, not by gfortran. With this update, GDB can now dereference pointers to objects of dynamic type, thereby correctly printing the dynamic Fortran arrays dereferenced from such pointers (as produced by the iFort compiler). ([BZ#514287](#)<sup>409</sup>)

- \* Debugging a program with thousands of set breakpoints was unacceptably slow. This was because a previous patch introduced a mechanism that hid breakpoint instructions and returned "shadow" content whenever `target_read_memory()` accessed memory. The aforementioned patch was implemented upstream to be used with a "breakpoint always-inserted" option, which was not implemented in Red Hat Enterprise Linux version of GDB. But Red Hat Enterprise Linux version backported it to solve a problem on Itanium where instruction (and thus even breakpoint instruction) boundaries are not byte-aligned. This update reimplements the shadowing functionality using more optimal  $\log(n)$  algorithm instead, which consequently prevents any unnecessary slowdown when processing programs with numerous set breakpoints. ([BZ#520618](#)<sup>410</sup>)

- \* GDB incorrectly skipped OpenMP parallel sections (instead of entering them as expected) when using the "next" command. This was caused by missing DWARF annotations from GCC that made it possible for OpenMP parallel sections to be incorrectly classified as function calls. To address this, GDB contains special instructions to make OpenMP parallel sections indifferent to normal code, allowing GDB to step into parallel sections with "next" correctly. ([BZ#533176](#)<sup>411</sup>)

- \* The GDB version banner now correctly displays "Red Hat Enterprise Linux" instead of "Fedora". ([BZ#537788](#)<sup>412</sup>)

<sup>407</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3546.html>

<sup>408</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=526533](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=526533)

<sup>409</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=514287](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=514287)

<sup>410</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=520618](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=520618)

<sup>411</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=533176](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=533176)

<sup>412</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=537788](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=537788)

- \* GDB no longer obsoletes the pstack package. ([BZ#550786](https://bugzilla.redhat.com/show_bug.cgi?id=550786)<sup>413</sup>)
- \* Loading symbols in STABS debug format could crash GDB. The STABS format is no longer supported, as Red Hat Enterprise Linux uses the debug format DWARF. With this update, loading symbols in STABS format no longer crashes GDB; instead, such symbols are simply loaded incorrectly. ([BZ#553672](https://bugzilla.redhat.com/show_bug.cgi?id=553672)<sup>414</sup>)
- \* Adding GDB support for Fortran modules in previous releases introduced a regression which prevented GDB from setting breakpoints on a Fortran program's name. This was caused by a bug in the search routines used when "set language fortran" is enabled. This update fixes the regression. ([BZ#559291](https://bugzilla.redhat.com/show_bug.cgi?id=559291)<sup>415</sup>)
- \* The Red Hat Enterprise Linux 5.5 version of GDB also contains a fix for an upstream GDB regression that prevented users from setting rwatch and awatch breakpoints before a program starts. This version of GDB implements a compatibility fix from GDB 6.8 to address the regression. ([BZ#562770](https://bugzilla.redhat.com/show_bug.cgi?id=562770)<sup>416</sup>)
- \* A "break-by-name on inlined functions" feature introduced in Fedora GDB made it possible for parameters of inlined functions to be incorrectly hidden. Whenever this occurred during debugging, GDB printed "<optimized out>" in backtraces or upon entering such functions. In some cases, stepping through inlined functions could also abort GDB with an internal error. This release resolves the issue by removing the "break-by-name on inlined functions" feature altogether. ([BZ#565601](https://bugzilla.redhat.com/show_bug.cgi?id=565601)<sup>417</sup>)

All GDB users should apply this update.

## 1.61. gfs-kmod

### 1.61.1. RHSA-2010:0291: Moderate security, bug fix and enhancement update

Updated gfs-kmod packages that fix one security issue, numerous bugs, and add one enhancement are now available for Red Hat Enterprise Linux 5.5, kernel release 2.6.18-194.el5.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

The gfs-kmod packages contain modules that provide the ability to mount and use GFS file systems.

A flaw was found in the gfs\_lock() implementation. The GFS locking code could skip the lock operation for files that have the S\_ISGID bit (set-group-ID on execution) in their mode set. A local, unprivileged user on a system that has a GFS file system mounted could use this flaw to cause a kernel panic. ([CVE-2010-0727](https://www.redhat.com/security/data/cve/CVE-2010-0727)<sup>418</sup>)

These updated gfs-kmod packages are in sync with the latest kernel (2.6.18-194.el5). The modules in earlier gfs-kmod packages failed to load because they did not match the running kernel. It was possible to force-load the modules. With this update, however, users no longer need to.

---

<sup>413</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=550786](https://bugzilla.redhat.com/show_bug.cgi?id=550786)

<sup>414</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=553672](https://bugzilla.redhat.com/show_bug.cgi?id=553672)

<sup>415</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=559291](https://bugzilla.redhat.com/show_bug.cgi?id=559291)

<sup>416</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=562770](https://bugzilla.redhat.com/show_bug.cgi?id=562770)

<sup>417</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=565601](https://bugzilla.redhat.com/show_bug.cgi?id=565601)

<sup>418</sup> <https://www.redhat.com/security/data/cve/CVE-2010-0727.html>

These updated gfs-kmod packages also fix the following bugs:

\* when SELinux was in permissive mode, a race condition during file creation could have caused one or more cluster nodes to be fenced and lock the remaining nodes out of the GFS file system. This race condition no longer occurs with this update. ([BZ#471258](https://bugzilla.redhat.com/show_bug.cgi?id=471258)<sup>419</sup>)

\* when ACLs (Access Control Lists) are enabled on a GFS file system, if a transaction that has started to do a write request does not have enough spare blocks for the operation it causes a kernel panic. This update ensures that there are enough blocks for the write request before starting the operation. ([BZ#513885](https://bugzilla.redhat.com/show_bug.cgi?id=513885)<sup>420</sup>)

\* requesting a "flock" on a file in GFS in either read-only or read-write mode would sometimes cause a "Resource temporarily unavailable" state error (error 11 for EWOULDBLOCK) to occur. In these cases, a flock could not be obtained on the file in question. This has been fixed with this update so that flocks can successfully be obtained on GFS files without this error occurring. ([BZ#515717](https://bugzilla.redhat.com/show_bug.cgi?id=515717)<sup>421</sup>)

\* the GFS withdraw function is a data integrity feature of GFS file systems in a cluster. If the GFS kernel module detects an inconsistency in a GFS file system following an I/O operation, the file system becomes unavailable to the cluster. The GFS withdraw function is less severe than a kernel panic, which would cause another node to fence the node. With this update, you can override the GFS withdraw function by mounting the file system with the "-o errors=panic" option specified. When this option is specified, any errors that would normally cause the system to withdraw cause the system to panic instead. This stops the node's cluster communications, which causes the node to be fenced. ([BZ#517145](https://bugzilla.redhat.com/show_bug.cgi?id=517145)<sup>422</sup>)

Finally, these updated gfs-kmod packages provide the following enhancement:

\* the GFS kernel modules have been updated to use the new generic freeze and unfreeze ioctl interface that is also supported by the following file systems: ext3, ext4, GFS2, JFS and ReiserFS. With this update, GFS supports freeze/unfreeze through the VFS-level FIFREEZE/FITHAW ioctl interface. ([BZ#487610](https://bugzilla.redhat.com/show_bug.cgi?id=487610)<sup>423</sup>)

Users are advised to upgrade to these latest gfs-kmod packages, updated for use with the 2.6.18-194.el5 kernel, which contain backported patches to correct these issues, fix these bugs, and add this enhancement.

## 1.62. gfs-utils

### 1.62.1. RHBA-2010:0290: bug fix update

Updated gfs-utils packages that fix various bugs are now available.

The gfs-utils packages provide the user-space tools necessary to mount, create, maintain and test GFS file systems.

The updated gfs-utils packages apply the following bug fixes:

---

<sup>419</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=471258](https://bugzilla.redhat.com/show_bug.cgi?id=471258)

<sup>420</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=513885](https://bugzilla.redhat.com/show_bug.cgi?id=513885)

<sup>421</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=515717](https://bugzilla.redhat.com/show_bug.cgi?id=515717)

<sup>422</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=517145](https://bugzilla.redhat.com/show_bug.cgi?id=517145)

<sup>423</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=487610](https://bugzilla.redhat.com/show_bug.cgi?id=487610)

\* GFS: gfs\_fsck sometimes needs to be run twice ([BZ#509225](https://bugzilla.redhat.com/show_bug.cgi?id=509225)<sup>424</sup>) \* gfs\_fsck cannot repair rindex problems when directly on block device ([BZ#512722](https://bugzilla.redhat.com/show_bug.cgi?id=512722)<sup>425</sup>) \* gfs\_fsck -n always returns 0 even if error is found ([BZ#508978](https://bugzilla.redhat.com/show_bug.cgi?id=508978)<sup>426</sup>)

All users of gfs-utils should upgrade to these updated packages, which resolve these issues.

## 1.63. gfs2-utils

### 1.63.1. RHBA-2010:0287: bug fix update

Updated gfs2-utils packages that fix various bugs are now available.

The gfs2-utils packages provide the user-space tools necessary to mount, create, maintain and test GFS2 file systems.

The updated gfs2-utils packages apply the following bug fixes:

gfs2\_edit segfault ([BZ#503485](https://bugzilla.redhat.com/show_bug.cgi?id=503485)<sup>427</sup>) gfs2\_edit produces unaligned access ([BZ#503530](https://bugzilla.redhat.com/show_bug.cgi?id=503530)<sup>428</sup>) fsck.gfs2: Message printed to stderr instead of stdout ([BZ#506682](https://bugzilla.redhat.com/show_bug.cgi?id=506682)<sup>429</sup>) gfs2\_tool man page incorrectly references gfs2\_mount ([BZ#514939](https://bugzilla.redhat.com/show_bug.cgi?id=514939)<sup>430</sup>) GFS2: fsck.gfs2 sometimes needs to be run twice ([BZ#500483](https://bugzilla.redhat.com/show_bug.cgi?id=500483)<sup>431</sup>) "fsck.gfs2: invalid option -- a" on boot when mounting root formatted as gfs2 ([BZ#507596](https://bugzilla.redhat.com/show_bug.cgi?id=507596)<sup>432</sup>) GFS2: gfs2\_fsck bugs found in rindex repair code ([BZ#514018](https://bugzilla.redhat.com/show_bug.cgi?id=514018)<sup>433</sup>) GFS2: gfs2\_edit fixes for 5.5 ([BZ#503529](https://bugzilla.redhat.com/show_bug.cgi?id=503529)<sup>434</sup>) gfs2-utils fails rebuild test ([BZ#515370](https://bugzilla.redhat.com/show_bug.cgi?id=515370)<sup>435</sup>) gfs2\_edit -p block# shows wrong height/offset on gfs1 and segfaults on gfs2 ([BZ#506343](https://bugzilla.redhat.com/show_bug.cgi?id=506343)<sup>436</sup>) fsck.gfs2 unable to fix some rindex corruption for block size < 4K ([BZ#520762](https://bugzilla.redhat.com/show_bug.cgi?id=520762)<sup>437</sup>) GFS2: gfs2\_edit savemeta not saving all extended attribute data ([BZ#527770](https://bugzilla.redhat.com/show_bug.cgi?id=527770)<sup>438</sup>) GFS2: fsck.gfs2 should fix the system statfs file ([BZ#539337](https://bugzilla.redhat.com/show_bug.cgi?id=539337)<sup>439</sup>) GFS2: gfs2\_edit savemeta bugs ([BZ#528786](https://bugzilla.redhat.com/show_bug.cgi?id=528786)<sup>440</sup>) quota file size not a multiple of struct gfs2\_quota ([BZ#536902](https://bugzilla.redhat.com/show_bug.cgi?id=536902)<sup>441</sup>) interrupted rgrp conversion does not allow re-converts ([BZ#548585](https://bugzilla.redhat.com/show_bug.cgi?id=548585)<sup>442</sup>) Conversion of inodes that are of different metatree heights in gfs and gfs2 is incorrect ([BZ#548588](https://bugzilla.redhat.com/show_bug.cgi?id=548588)<sup>443</sup>) Allow fsck.gfs2 to check RO mounted file systems ([BZ#557128](https://bugzilla.redhat.com/show_bug.cgi?id=557128)<sup>444</sup>) GFS2: gfs2\_convert should fix statfs file ([BZ#556961](https://bugzilla.redhat.com/show_bug.cgi?id=556961)<sup>445</sup>) gfs2\_convert doesn't convert jdata files correctly ([BZ#545602](https://bugzilla.redhat.com/show_bug.cgi?id=545602)<sup>446</sup>) GFS2: fatal: invalid metadata block after gfs2\_grow ([BZ#546683](https://bugzilla.redhat.com/show_bug.cgi?id=546683)<sup>447</sup>)

---

<sup>424</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=509225](https://bugzilla.redhat.com/show_bug.cgi?id=509225)

<sup>425</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=512722](https://bugzilla.redhat.com/show_bug.cgi?id=512722)

<sup>426</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=508978](https://bugzilla.redhat.com/show_bug.cgi?id=508978)

<sup>427</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=503485](https://bugzilla.redhat.com/show_bug.cgi?id=503485)

<sup>428</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=503530](https://bugzilla.redhat.com/show_bug.cgi?id=503530)

<sup>429</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=506682](https://bugzilla.redhat.com/show_bug.cgi?id=506682)

<sup>430</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=514939](https://bugzilla.redhat.com/show_bug.cgi?id=514939)

<sup>431</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=500483](https://bugzilla.redhat.com/show_bug.cgi?id=500483)

<sup>432</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=507596](https://bugzilla.redhat.com/show_bug.cgi?id=507596)

<sup>433</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=514018](https://bugzilla.redhat.com/show_bug.cgi?id=514018)

<sup>434</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=503529](https://bugzilla.redhat.com/show_bug.cgi?id=503529)

<sup>435</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=515370](https://bugzilla.redhat.com/show_bug.cgi?id=515370)

<sup>436</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=506343](https://bugzilla.redhat.com/show_bug.cgi?id=506343)

<sup>437</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=520762](https://bugzilla.redhat.com/show_bug.cgi?id=520762)

<sup>438</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=527770](https://bugzilla.redhat.com/show_bug.cgi?id=527770)

<sup>439</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=539337](https://bugzilla.redhat.com/show_bug.cgi?id=539337)

<sup>440</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=528786](https://bugzilla.redhat.com/show_bug.cgi?id=528786)

<sup>441</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=536902](https://bugzilla.redhat.com/show_bug.cgi?id=536902)

<sup>442</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=548585](https://bugzilla.redhat.com/show_bug.cgi?id=548585)

<sup>443</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=548588](https://bugzilla.redhat.com/show_bug.cgi?id=548588)

<sup>444</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=557128](https://bugzilla.redhat.com/show_bug.cgi?id=557128)

<sup>445</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=556961](https://bugzilla.redhat.com/show_bug.cgi?id=556961)

<sup>446</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=545602](https://bugzilla.redhat.com/show_bug.cgi?id=545602)

All users of gfs2-utils should upgrade to these updated packages, which resolve these issues.

## 1.64. glibc

### 1.64.1. RHBA-2009:1634: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1634](#)<sup>448</sup>

Updated glibc packages that resolve several issues are now available.

The glibc packages contain the standard C libraries used by multiple programs on the system. These packages contains the standard C and the standard math libraries. Without these two libraries, the Linux system cannot function properly.

These updated glibc packages provide fixes for the following bugs:

\* when a thread calls the `setuid()` function, the change of credentials needs to be performed in every thread as per POSIX requirements. This update corrects the implementation to avoid a race condition which occurred when a thread terminated or a new thread was created while the credential change was performed. ([BZ#533213](#)<sup>449</sup>)

\* the implementation of the `seg_timedwait()` function, in assembler, incorrectly decremented the number of waiting threads stored in a block of memory when an invalid nanosecond value was passed through its second argument. This error is corrected in this update. ([BZ#540475](#)<sup>450</sup>)

All users of glibc are advised to upgrade to these updated packages, which resolve these issues.

### 1.64.2. RHBA-2010:0050: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2010:0050](#)<sup>451</sup>

Updated glibc packages that fix a race condition while loading shared libraries are now available

The glibc packages contain the standard C libraries used by multiple programs on the system. These packages contains the standard C and the standard math libraries. Without these two libraries, the Linux system cannot function properly.

These updated glibc packages provide a fix for the following bug:

<sup>447</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=546683](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=546683)

<sup>449</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=533213](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=533213)

<sup>450</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=540475](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=540475)



\* a rarely-encountered and difficult-to-reproduce race condition existed between resolving dynamic symbols and loading shared libraries that could have resulted in library dependencies not being resolved. This update provides a fix that avoids the potential race condition. ([BZ#548692](https://bugzilla.redhat.com/show_bug.cgi?id=548692)<sup>452</sup>)

All users are advised to upgrade to these updated packages, which resolve this issue.

### 1.64.3. RHBA-2010:0306: bug fix and enhancement update

Updated glibc packages that fix several bugs and add an enhancement are now available.

The glibc packages contain the standard C libraries used by multiple programs on the system. These packages contain the standard C and the standard math libraries. Without these two libraries, the Linux system cannot function properly.

This update applies the following bug fixes:

\* a race condition with `seteuid()` occurred between the threads that run on starting the program, presenting the error "EUID is already set!" within 10 to 15 seconds. These updates provide exclusive processes running with no error on startup. ([BZ#491995](https://bugzilla.redhat.com/show_bug.cgi?id=491995)<sup>453</sup> and [BZ#522528](https://bugzilla.redhat.com/show_bug.cgi?id=522528)<sup>454</sup>)

\* assembler implementation of `sem_timedwait()` on x86/x86\_64 wrongly decrements the number of waiting threads stored in block of memory pointed to by (`sem_t *`) when an invalid nanosecond argument is used. This fix allows the correct nanosecond argument to be passed through the second argument. ([BZ#529997](https://bugzilla.redhat.com/show_bug.cgi?id=529997)<sup>455</sup>)

\* a race condition in glibc, between `_dl_lookup_symbol_x()` and `dlopen/dlclose/etc`, resulted in a failure in resolving dependencies. These updates provide for processes that are exclusive. ([BZ#547631](https://bugzilla.redhat.com/show_bug.cgi?id=547631)<sup>456</sup>)

This update also adds the following enhancement:

\* glibc: incorporates a number of tests to detect corruption in data structures used for heap memory allocation (`malloc/free`). This corruption can be caused deliberately by attackers exploiting buffer overflow vulnerabilities. This enhancement provides additional corruption tests. ([BZ#530107](https://bugzilla.redhat.com/show_bug.cgi?id=530107)<sup>457</sup>)

All users are advised to upgrade to this updated package, which resolves these issues and adds this enhancement.

## 1.65. gnome-vfs2

### 1.65.1. RHBA-2010:0317: bug fix update

An updated gnome-vfs2 package that fixes a bug is now available.

GNOME VFS is the GNOME virtual file system. It is the foundation of the Nautilus file manager. It provides a modular architecture and ships with several modules that implement support for file systems, http, ftp, and others. It provides a URI-based API, backend supporting asynchronous file operations, a MIME type manipulation library, and other features.

---

<sup>452</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=548692](https://bugzilla.redhat.com/show_bug.cgi?id=548692)

<sup>453</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=491995](https://bugzilla.redhat.com/show_bug.cgi?id=491995)

<sup>454</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=522528](https://bugzilla.redhat.com/show_bug.cgi?id=522528)

<sup>455</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=529997](https://bugzilla.redhat.com/show_bug.cgi?id=529997)

<sup>456</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=547631](https://bugzilla.redhat.com/show_bug.cgi?id=547631)

<sup>457</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=530107](https://bugzilla.redhat.com/show_bug.cgi?id=530107)



\* the `gnome-vfs2` package would only work correctly on a system running Samba 3.0 packages, and could not be installed on a system running Samba 3.3 packages. The version of `gnome-vfs` provided with this advisory depends only on a small Samba subpackage, which is independent from other Samba packages. The `gnome-vfs2` package can now be installed on a system running Samba 3.3 packages. ([BZ#555642](#)<sup>458</sup>)

Users are advised to check the parallel Samba advisory RHBA-2009:9287.

Users are advised to upgrade to this updated `gnome-vfs2` package, which resolves this issue.

## 1.65.2. RHBA-2010:0032: bug fix update



### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2010:0032](#)<sup>459</sup>

Updated `gnome-vfs2` packages that resolve several issues are now available.

GNOME VFS is the GNOME virtual file system. It is the foundation of the Nautilus file manager. It provides a modular architecture, and ships with several modules that implement support for file systems and protocols such as HTTP and FTP, among others.

These updated `gnome-vfs2` packages provide fixes for the following bugs:

\* an unresolved symbol in the `gnome-vfs2` library caused the system-config-network GUI application to be unable to start. ([BZ#247522](#)<sup>460</sup>)

\* client applications which used the `gnome-vfs2` library were unable to search for certain paths because the search process ended as soon as it encountered a file or directory which it was unable to read. This update fixes this bug in `gnome-vfs2` so that searches skip over unreadable files or directories and continue as expected.

Note: a future `nautilus` update will be released that properly fixes this bug in the Nautilus file manager. ([BZ#432764](#)<sup>461</sup>)

\* when attempting to move one or more files between two NFS mounts, the Nautilus file manager displayed a dialog box that stated: Error: "Not on the same file system." This error was caused by an EXDEV error in the `gnome-vfs2` file module due to rename semantics. With this update, moving a file from one NFS mount to another succeeds as expected due to the implementation of a proper copy-and-delete fallback routine. ([BZ#438116](#)<sup>462</sup>)

\* attempting to open a supported document type represented by a symbolic link on an NFS share with the Evince document viewer failed with the following error message:

Unable to open document Unhandled MIME type: "application/octet-stream"

<sup>458</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=555642](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=555642)

<sup>460</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=247522](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=247522)

<sup>461</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=432764](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=432764)

<sup>462</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=438116](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=438116)

This update improves this behavior with a symbolic link check so that Evince is now able to successfully open a link to a supported document type when both the link and actual file are located on an NFS share. ([BZ#481593](#)<sup>463</sup>)

\* the `gnome-vfs-daemon` service reads the list of mounted devices at `/proc/mounts` upon startup. If one of the device paths was not valid UTF-8, `gnome-vfs-daemon` was disconnected by D-Bus when it attempted to communicate the path over the system message bus, at which time it exited. However, other GNOME applications would then attempt to restart `gnome-vfs-daemon`, at which time the same sequence of events reoccurred, leading to a potentially infinite loop and much extraneous CPU usage. With this update, `gnome-vfs-daemon` correctly converts the information provided by `/proc/mounts` into valid UTF-8 before communicating it via D-Bus, which prevents the possibility of `gnome-vfs-daemon` being disconnected, exiting, and being restarted in a continuous fashion. ([BZ#486286](#)<sup>464</sup>)

\* accessing a WebDAV share which contained a comma in its path name with the Nautilus file manager resulted in a "File not found" error. This update ensures that reserved characters in path names are properly escaped, and thus Nautilus is able to access such paths as expected. ([BZ#503112](#)<sup>465</sup>)

All GNOME users are advised to upgrade to these updated packages, which resolve these issues. Running GNOME sessions must be restarted for the update to take effect.

## 1.66. gpart

### 1.66.1. RHBA-2009:1606: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2009:1606](#)<sup>466</sup>

A `gpart` update that fixes a bug in the `-debuginfo` package is now available.

`gpart` is a small tool which tries to guess what partitions are on a PC type harddisk in case the primary partition table was damaged.

This update addresses the following issue:

\* although `gpart` contains ELF objects, the `gpart-debuginfo` package was empty. With this update the `-debuginfo` package contains valid debugging information as expected. ([BZ#500598](#)<sup>467</sup>)

`gpart` users needing the `gpart debuginfo` package should install this upgraded package which fixes this problem.

---

<sup>463</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=481593](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=481593)

<sup>464</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=486286](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=486286)

<sup>465</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=503112](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=503112)

<sup>467</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=500598](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=500598)

## 1.67. gzip

### 1.67.1. RHSA-2010:0061: Moderate security update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2010:0061](#)<sup>468</sup>

An updated gzip package that fixes one security issue is now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The gzip package provides the GNU gzip data compression program.

An integer underflow flaw, leading to an array index error, was found in the way gzip expanded archive files compressed with the Lempel-Ziv-Welch (LZW) compression algorithm. If a victim expanded a specially-crafted archive, it could cause gzip to crash or, potentially, execute arbitrary code with the privileges of the user running gzip. This flaw only affects 64-bit systems. ([CVE-2010-0001](#)<sup>469</sup>)

Red Hat would like to thank Aki Helin of the Oulu University Secure Programming Group for responsibly reporting this flaw.

Users of gzip should upgrade to this updated package, which contains a backported patch to correct this issue.

## 1.68. hal

### 1.68.1. RHBA-2010:0256: bug fix update

Updated hal packages that fix various bugs are now available.

HAL is a daemon for collecting and maintaining information relating to hardware from several system sources.

The updated packages fix the following bugs:

- \* a sanity check in the HAL init script was incorrectly exiting with error code 0 when the script could not locate `/usr/sbin/hald`. The updated packages now contain a stronger sanity check, which returns the correct error code for a given condition. ([BZ#238113](#)<sup>470</sup>)
- \* a missing FDI quirk parameter for IBM X31 laptops prevented the laptop monitor from switching off during suspension. The updated packages add an extra "merge" element to the X40/X30 FDI definition, which correctly sets the `dpms_suspend` power management attribute. ([BZ#395991](#)<sup>471</sup>)
- \* a suspend hotkey combination (Fn+F1) used on Dell Latitude hardware was not mapped correctly. While the keycode sequence could be set manually, owners of Dell Latitude equipment experienced

<sup>469</sup> <https://www.redhat.com/security/data/cve/CVE-2010-0001.html>

<sup>470</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=238113](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=238113)

<sup>471</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=395991](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=395991)

unnecessary inconvenience when attempting to suspend using the hotkey combination. The updated packages add the correct mapping rules, which enable the Fn+F1 key combination. ([BZ#450326](https://bugzilla.redhat.com/show_bug.cgi?id=450326)<sup>472</sup>)

\* when HAL checked for ttyS devices, it would abend if `/sys/class/tty/ttyS*` existed but `/dev/ttyS*` was removed or modified. Customers using two or more PCI serial port boards (with port extension) often implemented scripts to rename the port labels on the hardware to match the `/dev/ttyS*` node. HAL checks did not correctly cater for this scenario. The updated packages check whether serial device nodes have been manually removed. ([BZ#486427](https://bugzilla.redhat.com/show_bug.cgi?id=486427)<sup>473</sup>)

\* a missing HAL video quirk setting prevented IBM 4838-310 POS units from resuming correctly from S3 suspend state. The updated packages include a `vbe_post` quirk that corrects the suspend issue. ([BZ#501726](https://bugzilla.redhat.com/show_bug.cgi?id=501726)<sup>474</sup>)

\* an incorrect parameter in `/etc/udev/rules.d/90-dm.rules` prevented LUKS-formatted (encrypted) USB disks from automounting using GNOME. Customers had to mount the drive manually, or comment out the `ignore_device` line in `90-dm.rules` to effect the change. The updated packages fully implement this workaround solution. ([BZ#519645](https://bugzilla.redhat.com/show_bug.cgi?id=519645)<sup>475</sup>)

\* a missing HAL suspend quirk parameter prevented owners of Lenovo ThinkPad T400 laptops (product key 2768A96) suspending and resuming a session from a previously suspended system. The issue presented on laptops with ATI Mobility Radeon HD 3400 Series chipsets (1002:95c4), or Intel Mobile 4 Series chipsets (8086:2a42). The updated packages fix the suspend issue by correctly specifying the `--quirk-vbe-post` option for T400 machines. ([BZ#571925](https://bugzilla.redhat.com/show_bug.cgi?id=571925)<sup>476</sup>)

All hal users are advised to upgrade to these updated packages, which resolve these issues.

## 1.69. hmacalc

### 1.69.1. RHBA-2010:0055: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2010:0055](https://bugzilla.redhat.com/show_bug.cgi?id=5055)<sup>477</sup>

An updated `hmacalc` package that fixes a self-test bug related to binary prelinking is now available.

The `hmacalc` package contains tools to calculate HMAC (Hash-based Message Authentication Code) values for files. The names and interfaces were designed to mimic those of the `sha1sum`, `sha256sum`, `sha384sum` and `sha512sum` tools provided by the `coreutils` package.

This updated `hmacalc` package fixes the following bug:

\* each time one of the tools in the `hmacalc` package is used, it performs a self-test by comparing the checksum of its own binary with the value which was computed when the binary package was built. However, if an `hmacalc` binary had been prelinked using the "prelink" command, and that command was not located in one of the directories listed in the `PATH` environment variable, then that binary

---

<sup>472</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=450326](https://bugzilla.redhat.com/show_bug.cgi?id=450326)

<sup>473</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=486427](https://bugzilla.redhat.com/show_bug.cgi?id=486427)

<sup>474</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=501726](https://bugzilla.redhat.com/show_bug.cgi?id=501726)

<sup>475</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=519645](https://bugzilla.redhat.com/show_bug.cgi?id=519645)

<sup>476</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=571925](https://bugzilla.redhat.com/show_bug.cgi?id=571925)

would be unable to use the prelink tool to verify the checksum against an unmodified copy of itself. This update contains a backported fix that allows hmacalc to remember the location of the prelink command that was available at build time, and to be able to use it if necessary.

Note that this fix is required in order to build the Linux kernel with FIPS-compliance (Federal Information Processing Standards) enabled. ([BZ#512275](#)<sup>478</sup>)

All users of hmacalc are advised to upgrade to this updated package, which resolves this issue.

## 1.70. httpd

### 1.70.1. RHSA-2010:0168: Moderate security and enhancement update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2010:0168](#)<sup>479</sup>

Updated httpd packages that fix two security issues and add an enhancement are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

The Apache HTTP Server is a popular web server.

It was discovered that `mod_proxy_ajp` incorrectly returned an "Internal Server Error" response when processing certain malformed requests, which caused the back-end server to be marked as failed in configurations where `mod_proxy` is used in load balancer mode. A remote attacker could cause `mod_proxy` to not send requests to back-end AJP (Apache JServ Protocol) servers for the retry timeout period (60 seconds by default) by sending specially-crafted requests. ([CVE-2010-0408](#)<sup>480</sup>)

A use-after-free flaw was discovered in the way the Apache HTTP Server handled request headers in subrequests. In configurations where subrequests are used, a multithreaded MPM (Multi-Processing Module) could possibly leak information from other requests in request replies. ([CVE-2010-0434](#)<sup>481</sup>)

This update also adds the following enhancement:

\* with the updated openssl packages from RHSA-2010:0162 installed, `mod_ssl` will refuse to renegotiate a TLS/SSL connection with an unpatched client that does not support RFC 5746. This update adds the "SSLInsecureRenegotiation" configuration directive. If this directive is enabled, `mod_ssl` will renegotiate insecurely with unpatched clients. ([BZ#567980](#)<sup>482</sup>)

Refer to the following Red Hat Knowledgebase article for more details about the changed `mod_ssl` behavior: <http://kbase.redhat.com/faq/docs/DOC-20491>

<sup>478</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=512275](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=512275)

<sup>480</sup> <https://www.redhat.com/security/data/cve/CVE-2010-0408.html>

<sup>481</sup> <https://www.redhat.com/security/data/cve/CVE-2010-0434.html>

<sup>482</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=567980](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=567980)

All httpd users should upgrade to these updated packages, which contain backported patches to correct these issues and add this enhancement. After installing the updated packages, the httpd daemon must be restarted for the update to take effect.

### 1.70.2. RHSA-2009:1579: Moderate security update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2009:1579](#)<sup>483</sup>

Updated httpd packages that fix multiple security issues are now available for Red Hat Enterprise Linux 3 and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The Apache HTTP Server is a popular Web server.

A flaw was found in the way the TLS/SSL (Transport Layer Security/Secure Sockets Layer) protocols handle session renegotiation. A man-in-the-middle attacker could use this flaw to prefix arbitrary plain text to a client's session (for example, an HTTPS connection to a website). This could force the server to process an attacker's request as if authenticated using the victim's credentials. This update partially mitigates this flaw for SSL sessions to HTTP servers using `mod_ssl` by rejecting client-requested renegotiation. ([CVE-2009-3555](#)<sup>484</sup>)

Note: This update does not fully resolve the issue for HTTPS servers. An attack is still possible in configurations that require a server-initiated renegotiation. Refer to the following Knowledgebase article for further information: <http://kbase.redhat.com/faq/docs/DOC-20491>

A NULL pointer dereference flaw was found in the Apache `mod_proxy_ftp` module. A malicious FTP server to which requests are being proxied could use this flaw to crash an httpd child process via a malformed reply to the EPSV or PASV commands, resulting in a limited denial of service. ([CVE-2009-3094](#)<sup>485</sup>)

A second flaw was found in the Apache `mod_proxy_ftp` module. In a reverse proxy configuration, a remote attacker could use this flaw to bypass intended access restrictions by creating a carefully-crafted HTTP Authorization header, allowing the attacker to send arbitrary commands to the FTP server. ([CVE-2009-3095](#)<sup>486</sup>)

All httpd users should upgrade to these updated packages, which contain backported patches to correct these issues. After installing the updated packages, the httpd daemon must be restarted for the update to take effect.

### 1.70.3. RHBA-2010:0252: bug fix and enhancement update

Updated httpd packages that fix bugs and add enhancements are now available.

The Apache HTTP Server is a popular and freely-available Web server.

---

<sup>484</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3555.html>

<sup>485</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3094.html>

<sup>486</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3095.html>

These updated httpd packages provide fixes for the following bugs:

- \* the mod\_authnz\_ldap module did not allow other modules to handle authorization if no LDAP-specific requirements were used in the "Require" directive. ([BZ#448350](#)<sup>487</sup>)
- \* the httpd "init" script did not work correctly if the PidFile directive was removed from httpd.conf. ([BZ#505002](#)<sup>488</sup>)
- \* mod\_ssl would fail to complete a handshake if more the 85 CAs were configured using SSLCACertificateFile and/or SSLCACertificatePath. ([BZ#510515](#)<sup>489</sup>)
- \* the "X-Pad" header used for compatibility with old browser implementations has been removed. ([BZ#526110](#)<sup>490</sup>)
- \* mod\_proxy\_ajp could fail if uploading large files. ([BZ#528640](#)<sup>491</sup>)
- \* .NET clients using the "Expect: 100-continue" header could cause spurious responses. ([BZ#533407](#)<sup>492</sup>)
- \* the OID() function supported in mod\_ssl's SSLRequire directive could not evaluate some extension types. ([BZ#552942](#)<sup>493</sup>)

The following enhancements have also been made:

- \* the "DiscardPathInfo" flag (or "DPI") has been added to mod\_rewrite. ([BZ#517500](#)<sup>494</sup>)
- \* the AuthLDAPRemoteUserAttribute directive has been added to mod\_authnz\_ldap. ([BZ#520838](#)<sup>495</sup>)
- \* the AuthLDAPDynamicGroups directive has been added to mod\_authnz\_ldap, to enable support for dynamic groups. ([BZ#252038](#)<sup>496</sup>)
- \* the mod\_substitute module is now included. ([BZ#539256](#)<sup>497</sup>)

All Apache users should install these updated packages which address these issues.

## 1.71. hwdata

### 1.71.1. RHEA-2010:0197: enhancement update

An updated hwdata package that adds various enhancements is now available.

The hwdata package contains tools for accessing and displaying hardware identification and configuration data.

This updated package adds entries for the following devices to the Red Hat Enterprise Linux 5.4 pci.ids and usb.ids databases:

---

<sup>487</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=448350](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=448350)

<sup>488</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=505002](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=505002)

<sup>489</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=510515](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=510515)

<sup>490</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=526110](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=526110)

<sup>491</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=528640](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=528640)

<sup>492</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=533407](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=533407)

<sup>493</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=552942](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=552942)

<sup>494</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=517500](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=517500)

<sup>495</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=520838](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=520838)

<sup>496</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=252038](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=252038)

<sup>497</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=539256](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=539256)



- \* Brocade 10G PCIe Ethernet Controller. ([BZ#475712](https://bugzilla.redhat.com/show_bug.cgi?id=475712)<sup>498</sup>)
- \* Sequel Imaging Calibrator. ([BZ#512050](https://bugzilla.redhat.com/show_bug.cgi?id=512050)<sup>499</sup>)
- \* Intel SerDes Gigabit Network Connection. ([BZ#517100](https://bugzilla.redhat.com/show_bug.cgi?id=517100)<sup>500</sup>)
- \* Intel 10 Gigabit Dual Port Backplane Connection. ([BZ#517131](https://bugzilla.redhat.com/show_bug.cgi?id=517131)<sup>501</sup>)
- \* Emulex OneConnect 10Gb iSCSI Initiator. ([BZ#529449](https://bugzilla.redhat.com/show_bug.cgi?id=529449)<sup>502</sup>)
- \* Emulex OneConnect 10Gb NIC. ([BZ#529453](https://bugzilla.redhat.com/show_bug.cgi?id=529453)<sup>503</sup>)
- \* Emulex OneConnect 10Gb FCoE Initiator. ([BZ#529455](https://bugzilla.redhat.com/show_bug.cgi?id=529455)<sup>504</sup>)
- \* Mellanox Infiniband NICs. ([BZ#529458](https://bugzilla.redhat.com/show_bug.cgi?id=529458)<sup>505</sup>)
- \* Intel Cougar Point. ([BZ#566852](https://bugzilla.redhat.com/show_bug.cgi?id=566852)<sup>506</sup>)
- \* NC375T PCI Express Quad Port Gigabit Server Adapter. ([BZ#569910](https://bugzilla.redhat.com/show_bug.cgi?id=569910)<sup>507</sup>)

Users of hwdata are advised to upgrade to this updated package, which adds these enhancements.

## 1.72. ia32el

### 1.72.1. RHBA-2010:0250: bug fix update

An ia32el update that fixes several bugs is now available.

ia32el is the IA-32 Execution Layer platform, which allows the emulation of IA-32 binaries on IA-64.

This updated package addresses the following issues:

- \* When using the `-D_FILE_OFFSET_BITS=64` compile option, the platform would try to call `syscall statfs64` (`syscall id=268`). Unfortunately, this was unsupported by the previous package. Instead, the platform would resort to `statfs()`, and the case would fail. This package adds support for `syscall statfs64`. The platform no longer resorts to `statfs()`, and works correctly. ([BZ#514938](https://bugzilla.redhat.com/show_bug.cgi?id=514938)<sup>508</sup>)
- \* When `SIGALRM` invokes the signal handler, the ia32el application that installed the signal handler stops executing system calls in the correct order. This package adds a patch to the code that changes the conditions for the order of executing system calls, preventing the signal handler from affecting it. ([BZ#515165](https://bugzilla.redhat.com/show_bug.cgi?id=515165)<sup>509</sup>)
- \* The ia32el did not pass the second, third and fourth offset arguments of the `fadvice64()` or `fadvice64_64()` system call methods to the kernel correctly because it was unable to handle 64-bit

---

<sup>498</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=475712](https://bugzilla.redhat.com/show_bug.cgi?id=475712)

<sup>499</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=512050](https://bugzilla.redhat.com/show_bug.cgi?id=512050)

<sup>500</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=517100](https://bugzilla.redhat.com/show_bug.cgi?id=517100)

<sup>501</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=517131](https://bugzilla.redhat.com/show_bug.cgi?id=517131)

<sup>502</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=529449](https://bugzilla.redhat.com/show_bug.cgi?id=529449)

<sup>503</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=529453](https://bugzilla.redhat.com/show_bug.cgi?id=529453)

<sup>504</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=529455](https://bugzilla.redhat.com/show_bug.cgi?id=529455)

<sup>505</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=529458](https://bugzilla.redhat.com/show_bug.cgi?id=529458)

<sup>506</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=566852](https://bugzilla.redhat.com/show_bug.cgi?id=566852)

<sup>507</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=569910](https://bugzilla.redhat.com/show_bug.cgi?id=569910)

<sup>508</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=514938](https://bugzilla.redhat.com/show_bug.cgi?id=514938)

<sup>509</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=515165](https://bugzilla.redhat.com/show_bug.cgi?id=515165)



arguments for that system call. This meant that the offset arguments were not recognized as valid by the kernel. Support for 64-bit arguments has now been added. ([BZ#528590](#)<sup>511510</sup>)

\* The `clock_nanosleep()` system call method's fourth argument (remaining time) retained old values when interrupted by signal (EINTR). This caused invalid values to return for this argument. This patch adds a validity check before the values are returned. ([BZ#528590](#)<sup>513512</sup>)

\* The ia32el would not perform operations on the third argument of the `sendfile()` system call method correctly. As a result, after a successful system call, the offset argument would not be set to the value of the byte following the last byte read. This updated package contains a patch to correctly set the offset argument (during the system call). ([BZ#528596](#)<sup>514</sup>)

\* The ia32el previously broke the arguments of the `sync_file_range()` syscall. When the syscall was run, it would respond with an 'Invalid argument' error. A patch has been created that fixes the syntax error in the code. The ia32el now reads the `sync_file_range()` arguments correctly. ([BZ#528597](#)<sup>515</sup>)

\* When a NULL pointer was specified for the 2nd argument of the `timer_create()` syscall, the ia32el would pass the kernel a non-NULL pointer to uninitialized data instead, and the syscall would fail. This package provides a patch that adjusts the syntax of the code for the `timer_create()` syscall, so that the ia32el correctly interprets the NULL pointer. ([BZ#528598](#)<sup>516</sup>)

\* The NOTE offset and filesize of some core dumps of i386 processes running under ia32el were greater than the first LOAD offset according to 'readelf -l'. When this happened, the gdb couldn't read the core file. This package includes a patch that adjusts the size of the offset to greater than that of the NOTE offset and filesize. The gdb can now successfully read the core file. ([BZ#533269](#)<sup>517</sup>)

Users are advised to upgrade to this updated ia32el package which resolves these issues.

## 1.73. iasl

### 1.73.1. RHBA-2010:0226: bug fix and enhancement update

An updated iasl package that fixes a bug and introduces a feature enhancement is now available.

iasl compiles ASL (ACPI Source Language) into AML (ACPI Machine Language), which is suitable for inclusion as a DSDT in system firmware. It also can disassemble AML, for debugging purposes.

\* the default version of iasl was old, and could not properly decode DMAR tables. This sometimes resulted in incorrect decoding. Updating to the latest version of the iasl package has corrected this behavior, and DMAR tables are now decoded correctly. ([BZ#518109](#)<sup>518</sup>)

\* the iasl package has been updated to the latest version. ([BZ#518209](#)<sup>519</sup>)

Users are advised to upgrade to this updated iasl package, which resolves this issue.

<sup>511</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=528590](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=528590)

<sup>510</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=528590](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=528590)

<sup>513</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=528590](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=528590)

<sup>512</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=528590](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=528590)

<sup>514</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=528596](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=528596)

<sup>515</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=528597](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=528597)

<sup>516</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=528598](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=528598)

<sup>517</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=533269](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=533269)

<sup>518</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=518109](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=518109)

<sup>519</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=518209](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=518209)

### 1.74. inn

#### 1.74.1. RHBA-2009:1509: bug fix update



##### Note

This update has already been released (prior to the GA of this release) as FASTRACK errata [RHBA-2009:1509](#)<sup>520</sup>

Updated inn packages that resolve an issue are now available.

INN (InterNetNews) is a complete system for serving Usenet news and private newsfeeds. INN includes innd, an NNTP (NetNews Transport Protocol) server, and nnrpd, a newsreader that is spawned for each client. Both innd and nnrpd vary slightly from the NNTP protocol, but not in ways that are easily noticed.

These updated packages address the following issue:

\* a PID file -- `/var/run/news/innd.pid` -- is created by the Internet News NNTP server, innd, at startup. If this file was not present when an attempt to stop innd was made, the service did not stop. With this update, the innd init script adds logic to stop innd with the `killproc` command if a "service innd stop" command is issued and `innd.pid` cannot be found. The updated init script also returns a message, "Stopping INN service (PID not found, the hard way)", in this case. ([BZ#464916](#)<sup>521</sup>)

All inn users are advised to upgrade to these updated packages, which resolve this issue.

### 1.75. iproute

#### 1.75.1. RHBA-2009:1520: bug fix update



##### Note

This update has already been released (prior to the GA of this release) as FASTRACK errata [RHBA-2009:1520](#)<sup>522</sup>

An updated iproute package that fixes a bug is now available.

The iproute package contains networking utilities such as `ip` and `rtmon`, which use the advanced networking capabilities of the Linux 2.4 and 2.6 kernels.

This update addresses the following problem:

\* if IPv6 was disabled, running the "ss" command resulted in a segmentation fault. A workaround was to run "ss -f inet". With this update the return value checks for `net_*_open` were fixed and the workaround is no longer necessary. The `ss` command again returns socket statistics as expected. ([BZ#493578](#)<sup>523</sup>)

---

<sup>521</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=464916](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=464916)

<sup>523</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=493578](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=493578)

All iproute users are advised to upgrade to this updated package, which resolves this issue.

## 1.76. iprutils

### 1.76.1. RHEA-2010:0229: enhancement update

An enhanced iprutils package is now available.

The iprutils package provides utilities to manage and configure SCSI devices that are supported by the ipr SCSI storage device driver.

This package upgrades iprutils to version 2.2.18, which includes:

\* support for the Generation 2 SAS (serial attached SCSI) PCI-E card with SSD (solid-state drive) has been added to systems with the PowerPC 64 architecture. ([BZ#512246](#)<sup>524</sup>)

\* iprconfig is a utility for configuring and recovering IBM Power RAID storage adapters. The iprconfig utility previously reported an incorrect firmware level for enclosures when called from a command line on systems with the PowerPC 64 architecture. The firmware level was reported correctly in the iprconfig graphical user interface (GUI). The iprconfig utility has been updated to handle SES (SCSI enclosure services) devices the same in both the command line and GUI, and the firmware level for enclosures is now reported correctly. ([BZ#532544](#)<sup>525</sup>)

Users with PowerPC 64 systems are advised to upgrade to this updated iprutils package, which adds these enhancements.

## 1.77. iptables

### 1.77.1. RHBA-2009:1539: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1539](#)<sup>526</sup>

Updated iptables packages that fix a bug are now available.

The iptables utility controls the network packet filtering code in the Linux kernel.

These updated packages fix the following bug:

\* the memory alignment of `ipt_connlimit_data` was incorrect on x86-based systems. This update adds an explicit aligned attribute to the `ipt_connlimit_data` struct to correct this. ([BZ#529687](#)<sup>527</sup>)

Users are advised to upgrade to these updated iptables packages, which resolve this issue.

<sup>524</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=512246](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=512246)

<sup>525</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=532544](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=532544)

<sup>527</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=529687](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=529687)

### 1.78. iptstate

#### 1.78.1. RHBA-2009:1676: bug fix update



##### Note

This update has already been released (prior to the GA of this release) as FASTRACK errata [RHBA-2009:1676](#)<sup>528</sup>

An updated iptstate package that resolves an issue is now available.

The iptstate utility displays the states held by your stateful firewall in a top-like manner.

This updated iptstate package fixes the following bug:

\* iptstate used a curses output function in single-run mode where curses is not used. Running "ipstate -s -S [address] -D [address]" caused ipstate to crash with a Segmentation Fault error. Note: running the command without the single-run mode switch (-s) did not crash. With this update, the bug is fixed and iptstate runs in single-run mode correctly, as expected. ([BZ#474381](#)<sup>529</sup>)

All iptstate users should upgrade to this updated package, which resolves this issue.

### 1.79. ipw2200-firmware

#### 1.79.1. RHEA-2010:0218: enhancement update

An enhanced ipw2200-firmware package is now available.

The ipw2200-firmware package contains the firmware files required by Intel PRO/Wireless 2200 network adapters.

The enhancement contains new open source 802.11a/bg drivers, which are compatible with ipw2200 drivers in the latest Red Hat Enterprise Linux kernels. ([BZ#494492](#)<sup>530</sup>)

Users with hardware containing Intel PRO/Wireless 2220 network adapters are advised to install this enhancement.

### 1.80. iscsi-initiator-utils

#### 1.80.1. RHBA-2010:0078: bug fix update



##### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2010:0078](#)<sup>531</sup>

---

<sup>529</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=474381](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=474381)

<sup>530</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=494492](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=494492)

An updated iscsi-initiator-utils package that fixes a bug is now available.

The iscsi-initiator-utils package provides the server daemon for the iSCSI protocol, as well as the utility programs used to manage it. iSCSI is a protocol for distributed disk access using SCSI commands sent over Internet Protocol networks.

This updated iscsi-initiator-utils package fixes the following bug:

\* removing the bnx2i module from the kernel, or running ifdown on the network interface being used by the bnx2i driver, and then reloading the kernel module or running ifup, did not result in automatic reconnection to SCSI sessions. As a workaround, the iscsid service had to be stopped and then restarted. With this update, SCSI sessions are automatically reconnected to after removing and reloading the bnx2i kernel module, or bringing the network interface down and then up again with ifdown and ifup. ([BZ#549629](https://bugzilla.redhat.com/show_bug.cgi?id=549629)<sup>532</sup>)

All users of iscsi-initiator-utils are advised to upgrade to this updated package, which resolves this issue.

## 1.80.2. RHBA-2010:0293: bug fix and enhancement update

An updated iscsi-initiator-utils package that fixes various bugs and provides new enhancements is now available.

The iscsi package provides the server daemon for the iSCSI protocol, as well as the utility programs used to manage it. iSCSI is a protocol for distributed disk access using SCSI commands sent over Internet Protocol networks.

The following bugs have been fixed in this release:

\* There was a problem with the discovery mechanism when iSCSI ifaces were used with different initiator names. The sendtarget discovery feature was using the default name (`/etc/iscsi/initiatorname.iscsi`) instead of the iname in the iface. As a consequence, the wrong name was being used. The discovery mechanism has now been fixed so that it uses the iname in the iface. As a result, they are discovered correctly and the right names are used. ([BZ#504666](https://bugzilla.redhat.com/show_bug.cgi?id=504666)<sup>533</sup>)

\* `chkconfig` was being run on service start to enable and disable services. This was causing a number of problems, as it was broken on read-only root systems and it also recalculated dependencies, causing a change of ordering in `/etc/rc` whilst the system is running. To fix this issue, `chkconfig` has been removed from the package so these issues will no longer occur as a result. ([BZ#511271](https://bugzilla.redhat.com/show_bug.cgi?id=511271)<sup>534</sup>)

\* Removing the `bnx2` modules or running `ifdown` on the network interface being used by `bnx2i` driver would result in the iSCSI sessions being disconnected. Reloading the module or running `ifup` would not reconnect the SCSI sessions. A patch has been added and, as a result, the iSCSI session now recovers after `iconfig` is brought down and back up. ([BZ#514926](https://bugzilla.redhat.com/show_bug.cgi?id=514926)<sup>535</sup>)

\* The iscsi initiator would fail to connect to a target when the `bnx2i` transport was being used. As a consequence, the log-in attempt would time out and fail. A fix has been made to the way in which MAC addresses are handled. As a result, users can now successfully log in. ([BZ#520508](https://bugzilla.redhat.com/show_bug.cgi?id=520508)<sup>536</sup>)

<sup>532</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=549629](https://bugzilla.redhat.com/show_bug.cgi?id=549629)

<sup>533</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=504666](https://bugzilla.redhat.com/show_bug.cgi?id=504666)

<sup>534</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=511271](https://bugzilla.redhat.com/show_bug.cgi?id=511271)

<sup>535</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=514926](https://bugzilla.redhat.com/show_bug.cgi?id=514926)

<sup>536</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=520508](https://bugzilla.redhat.com/show_bug.cgi?id=520508)

\* There was a small typographical error in the `/usr/session_info.c` print out, where "REOPEN" was incorrectly spelled as "REPOEN". This has now been corrected and the correctly spelled version of the word is output as a result. ([BZ#531748](#)<sup>537</sup>).

The following enhancements have also been added in this release:

\* The Broadcom iSCSI user-space components have been updated to support ipv6 and 10G components. As a result, a broader range of hardware is now supported. ([BZ#517380](#)<sup>538</sup>)

\* The `/etc/init.d/iscsid` file has been patched in order to support the ServerEngines be2iscsi driver. As a result, this hardware is now available for utilization. ([BZ#556984](#)<sup>539</sup>)

Users are advised to upgrade to this updated `iscsi-initiator-utils` package, which resolve these issues.

## 1.81. iwl3945-firmware

### 1.81.1. RHEA-2010:0219: enhancement update

An enhanced `iwl3945-firmware` package that works with the `iwlwifi-3945` driver in the latest Red Hat Enterprise Linux kernel to enable support for the Intel PRO/Wireless 3945ABG/BG Network Connection Adapter is now available.

`iwlwifi-3945` is a kernel driver module for the Intel PRO/Wireless 3945ABG/BG Network Connection Adapter (aka `iwl3945` hardware). The `iwlwifi-3945` driver requires firmware loaded on the device in order to function. The `iwl3945-firmware` package provides the `iwl3945` driver with this required firmware and enables the driver to function correctly with `iwl3945` hardware.

This updated `iwl3945-firmware` package adds the following enhancement:

\* it is best to pair equivalent versions of these components in order to provide maximum compatibility between them. This update brings the firmware into line with the kernel driver included in the latest Red Hat Enterprise Linux kernel. ([BZ#534100](#)<sup>540</sup>)

Intel PRO/Wireless 3945ABG/BG Network Connection Adapter users using the `iwl3945` driver should upgrade to this updated package, which adds this enhancement.

## 1.82. iwl4965-firmware

### 1.82.1. RHEA-2010:0215: enhancement update

An enhanced `iwl4965-firmware` package is now available.

This package contains the firmware required by the `iwl4965` driver for Linux.

\* The firmware package has been enhanced to synchronize it with the latest version of the upstream Intel Wireless Wi-Fi Link 4965AGN driver (version 228.61.2.24). This upgrade brings about the following new functionality:

---

<sup>537</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=531748](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=531748)

<sup>538</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=517380](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=517380)

<sup>539</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=556984](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=556984)

<sup>540</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=534100](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=534100)

More graceful handling of Rx hangs (NMI) More reliable scanning A ten second pauses after association before power-down Receiver is now reset via re-tune after it misses beacons TGK measurement is now disabled when it receives a packet More reliable Tx with ACK/BA/CTS

As a result, the driver is now more reliable in a range of areas, scanning more efficiently and handling problems and interruptions better. ([BZ#510757](#)<sup>541</sup>)

Users are advised to upgrade to this updated iwl4965-firmware package, which resolves this issue.

## 1.83. iwl5000-firmware

### 1.83.1. RHEA-2010:0216: enhancement update

An updated iwl5000-firmware package is now available.

The iwl5000-firmware package provides the iwlmn wireless driver with the firmware it requires in order to function correctly with iwlmn hardware.

This updated iwl5000-firmware package adds the following enhancement:

\* the iwlmn driver and the iwl5000 firmware work together to provide proper wireless functionality. It is best to pair equivalent versions of these components in order to provide maximum compatibility between them, which this updated package provides. ([BZ#501609](#)<sup>542</sup>)

Users of wireless devices which use iwl5000 firmware are advised to upgrade to this updated package, which adds this enhancement.

## 1.84. java-1.6.0-ibm

### 1.84.1. RHBA-2010:0327: bug fix update

Updated java-1.6.0-ibm packages that fix an issue with time zone information are now available for Red Hat Enterprise Linux 5 Supplementary.

IBM's 1.6.0 Java release includes the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit.

These updated java-1.6.0-ibm packages fix a bug where the IBM Java 6 Runtime Environment did not recognize several time zones. ([BZ#569623](#)<sup>543</sup>)

All users of java-1.6.0-ibm are advised to upgrade to these updated packages, which contain new time zone data and therefore resolve this issue.

---

<sup>541</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=510757](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=510757)

<sup>542</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=501609](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=501609)

<sup>543</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=569623](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=569623)



## 1.85. java-1.6.0-openjdk

### 1.85.1. RHSA-2009:1584: Important security update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2009:1584](#)<sup>544</sup>

Updated java-1.6.0-openjdk packages that fix several security issues are now available for Red Hat Enterprise Linux 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

These packages provide the OpenJDK 6 Java Runtime Environment and the OpenJDK 6 Software Development Kit. The Java Runtime Environment (JRE) contains the software and tools that users need to run applications written using the Java programming language.

An integer overflow flaw and buffer overflow flaws were found in the way the JRE processed image files. An untrusted applet or application could use these flaws to extend its privileges, allowing it to read and write local files, as well as to execute local applications with the privileges of the user running the applet or application. ([CVE-2009-3869](#)<sup>545</sup>, [CVE-2009-3871](#)<sup>546</sup>, [CVE-2009-3873](#)<sup>547</sup>, [CVE-2009-3874](#)<sup>548</sup>)

An information leak was found in the JRE. An untrusted applet or application could use this flaw to extend its privileges, allowing it to read and write local files, as well as to execute local applications with the privileges of the user running the applet or application. ([CVE-2009-3881](#)<sup>549</sup>)

It was discovered that the JRE still accepts certificates with MD2 hash signatures, even though MD2 is no longer considered a cryptographically strong algorithm. This could make it easier for an attacker to create a malicious certificate that would be treated as trusted by the JRE. With this update, the JRE disables the use of the MD2 algorithm inside signatures by default. ([CVE-2009-2409](#)<sup>550</sup>)

A timing attack flaw was found in the way the JRE processed HMAC digests. This flaw could aid an attacker using forged digital signatures to bypass authentication checks. ([CVE-2009-3875](#)<sup>551</sup>)

Two denial of service flaws were found in the JRE. These could be exploited in server-side application scenarios that process DER-encoded (Distinguished Encoding Rules) data. ([CVE-2009-3876](#)<sup>552</sup>, [CVE-2009-3877](#)<sup>553</sup>)

An information leak was found in the way the JRE handled color profiles. An attacker could use this flaw to discover the existence of files outside of the color profiles directory. ([CVE-2009-3728](#)<sup>554</sup>)

---

<sup>545</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3869.html>

<sup>546</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3871.html>

<sup>547</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3873.html>

<sup>548</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3874.html>

<sup>549</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3881.html>

<sup>550</sup> <https://www.redhat.com/security/data/cve/CVE-2009-2409.html>

<sup>551</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3875.html>

<sup>552</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3876.html>

<sup>553</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3877.html>

<sup>554</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3728.html>



A flaw in the JRE with passing arrays to the X11GraphicsDevice API was found. An untrusted applet or application could use this flaw to access and modify the list of supported graphics configurations. This flaw could also lead to sensitive information being leaked to unprivileged code. ([CVE-2009-3879](#)<sup>555</sup>)

It was discovered that the JRE passed entire objects to the logging API. This could lead to sensitive information being leaked to either untrusted or lower-privileged code from an attacker-controlled applet which has access to the logging API and is therefore able to manipulate (read and/or call) the passed objects. ([CVE-2009-3880](#)<sup>556</sup>)

Potential information leaks were found in various mutable static variables. These could be exploited in application scenarios that execute untrusted scripting code. ([CVE-2009-3882](#)<sup>557</sup>, [CVE-2009-3883](#)<sup>558</sup>)

An information leak was found in the way the `TimeZone.getTimeZone` method was handled. This method could load time zone files that are outside of the `[JRE_HOME]/lib/zi/` directory, allowing a remote attacker to probe the local file system. ([CVE-2009-3884](#)<sup>559</sup>)

Note: The flaws concerning applets in this advisory, [CVE-2009-3869](#)<sup>560</sup>, [CVE-2009-3871](#)<sup>561</sup>, [CVE-2009-3873](#)<sup>562</sup>, [CVE-2009-3874](#)<sup>563</sup>, [CVE-2009-3879](#)<sup>564</sup>, [CVE-2009-3880](#)<sup>565</sup>, [CVE-2009-3881](#)<sup>566</sup> and [CVE-2009-3884](#)<sup>567</sup>, can only be triggered in `java-1.6.0-openjdk` by calling the "appletviewer" application.

All users of `java-1.6.0-openjdk` are advised to upgrade to these updated packages, which resolve these issues. All running instances of OpenJDK Java must be restarted for the update to take effect.

## 1.86. java-1.6.0-sun

### 1.86.1. RHBA-2010:0072: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2010:0072](#)<sup>568</sup>

Updated `java-1.6.0-sun` packages are now available for Red Hat Enterprise Linux 5.4 Supplementary.

The `java-1.6.0-sun` packages include the Sun Java 6 Runtime Environment, Sun Java 6 Software Development Kit (SDK), the source code for the Sun Java class libraries, the Sun Java browser plug-in and Web Start, the Sun JDBC/ODBC bridge driver, and demonstration files for the Sun Java 6 SDK.

<sup>555</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3879.html>

<sup>556</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3880.html>

<sup>557</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3882.html>

<sup>558</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3883.html>

<sup>559</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3884.html>

<sup>560</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3869.html>

<sup>561</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3871.html>

<sup>562</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3873.html>

<sup>563</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3874.html>

<sup>564</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3879.html>

<sup>565</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3880.html>

<sup>566</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3881.html>

<sup>567</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3884.html>

These updated java-1.6.0-sun packages upgrade Sun's Java 6 SDK from version 1.6.0\_17 to version 1.6.0\_18, which provides fixes for a number of bugs. To view the release notes for the bug fixes included in this update, refer to the URL provided in the "References" section of this errata. ([BZ#557418](#)<sup>569</sup>)

All users of java-1.6.0-sun are advised to upgrade to these updated packages, which resolve these issues.

## 1.87. kdelibs

### 1.87.1. RHBA-2009:1464: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1464](#)<sup>570</sup>

Updated kdelibs packages that fix the bugs are now available.

The kdelibs packages contain a set of common libraries used by all applications written for the K Desktop Environment (KDE). kdelibs includes kdecore (KDE core library); kdeui (user interface); kfm (file manager); khtmlw (HTML widget); kio (input/output and networking); kspell (spelling checker); jscript (javascript); kab (addressbook); and kimgio (image manipulation).

This update addresses the following issue:

\* the kde.sh shell script used the keyword "source". The pdksh (Public Domain Korn SHell) package, a new package in Red Hat Enterprise Linux 5.4, does not recognize the "source" keyword in shell scripts. Consequently, if pdksh was used as the shell on systems with KDE installed, the following error message was returned in login shells:

```
ksh: /etc/profile.d/kde.sh[7]: source: not found
```

The kde.sh shell script in this update has been edited with "source" replaced by "." The full stop keyword (.) is an alias for "source" in Bourne-compatible shells, including pdksh. Once installed, KDE users running the pdksh shell will no longer get the above error message. ([BZ#523968](#)<sup>571</sup>)

Note: this bug was a known issue at the release of Red Hat Enterprise Linux 5.4 and a manual version of the fix included in this update was documented in the Red Hat Enterprise Linux 5.4 Technical Notes:

[http://redhat.com/docs/en-US/Red\\_Hat\\_Enterprise\\_Linux/5.4/html/Technical\\_Notes/Known\\_Issues-pdksh.html](http://redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/5.4/html/Technical_Notes/Known_Issues-pdksh.html)

If /etc/profile.d/kde.sh already exists, the new version included with this update is installed as /etc/profile.d/kde.sh.rpmnew.

Therefore, on systems where an extant kde.sh has been manually edited as per the Red Hat Enterprise Linux 5.4 Technical Notes, the manual fix is retained.

---

<sup>569</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=557418](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=557418)

<sup>571</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=523968](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=523968)

On systems where `kde.sh` already exists and the workaround has not been applied, however, installing this update does not, of itself, implement the fix. After installation on such systems, renaming `kde.sh` and `kde.sh.rpmnew` as follows will implement the fix:

```
cp /etc/profile.d/kde.sh /etc/profile.d/kde.sh.bak cp /etc/profile.d/kde.sh.rpmnew /etc/profile.d/kde.sh
```

All KDE and `pdksh` users should install this updated package which fixes this bug.

## 1.87.2. RHSA-2009:1601: Critical security update



### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2009:1601](#)<sup>572</sup>

Updated `kdelibs` packages that fix one security issue are now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having critical security impact by the Red Hat Security Response Team.

The `kdelibs` packages provide libraries for the K Desktop Environment (KDE).

A buffer overflow flaw was found in the `kdelibs` string to floating point conversion routines. A web page containing malicious JavaScript could crash Konqueror or, potentially, execute arbitrary code with the privileges of the user running Konqueror. ([CVE-2009-0689](#)<sup>573</sup>)

Users should upgrade to these updated packages, which contain a backported patch to correct this issue. The desktop must be restarted (log out, then log back in) for this update to take effect.

## 1.88. kernel

### 1.88.1. RHSA-2010:0147: Important security and bug fix update



### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2010:0147](#)<sup>574</sup>

Updated kernel packages that fix multiple security issues and several bugs are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

<sup>573</sup> <https://www.redhat.com/security/data/cve/CVE-2009-0689.html>

### Security fixes:

- \* a NULL pointer dereference flaw was found in the `sctp_rcv_ootb()` function in the Linux kernel Stream Control Transmission Protocol (SCTP) implementation. A remote attacker could send a specially-crafted SCTP packet to a target system, resulting in a denial of service. ([CVE-2010-0008](https://www.redhat.com/security/data/cve/CVE-2010-0008.html)<sup>575</sup>, Important)
- \* a missing boundary check was found in the `do_move_pages()` function in the memory migration functionality in the Linux kernel. A local user could use this flaw to cause a local denial of service or an information leak. ([CVE-2010-0415](https://www.redhat.com/security/data/cve/CVE-2010-0415.html)<sup>576</sup>, Important)
- \* a NULL pointer dereference flaw was found in the `ip6_dst_lookup_tail()` function in the Linux kernel. An attacker on the local network could trigger this flaw by sending IPv6 traffic to a target system, leading to a system crash (kernel OOPS) if `dst->neighbour` is NULL on the target system when receiving an IPv6 packet. ([CVE-2010-0437](https://www.redhat.com/security/data/cve/CVE-2010-0437.html)<sup>577</sup>, Important)
- \* a NULL pointer dereference flaw was found in the ext4 file system code in the Linux kernel. A local attacker could use this flaw to trigger a local denial of service by mounting a specially-crafted, journal-less ext4 file system, if that file system forced an EROFS error. ([CVE-2009-4308](https://www.redhat.com/security/data/cve/CVE-2009-4308.html)<sup>578</sup>, Moderate)
- \* an information leak was found in the `print_fatal_signal()` implementation in the Linux kernel. When `"/proc/sys/kernel/print-fatal-signals"` is set to 1 (the default value is 0), memory that is reachable by the kernel could be leaked to user-space. This issue could also result in a system crash. Note that this flaw only affected the i386 architecture. ([CVE-2010-0003](https://www.redhat.com/security/data/cve/CVE-2010-0003.html)<sup>579</sup>, Moderate)
- \* missing capability checks were found in the ebttables implementation, used for creating an Ethernet bridge firewall. This could allow a local, unprivileged user to bypass intended capability restrictions and modify ebttables rules. ([CVE-2010-0007](https://www.redhat.com/security/data/cve/CVE-2010-0007.html)<sup>580</sup>, Low)

### Bug fixes:

- \* a bug prevented Wake on LAN (WoL) being enabled on certain Intel hardware. ([BZ#543449](https://bugzilla.redhat.com/show_bug.cgi?id=543449)<sup>581</sup>)
- \* a race issue in the Journaling Block Device. ([BZ#553132](https://bugzilla.redhat.com/show_bug.cgi?id=553132)<sup>582</sup>)
- \* programs compiled on x86, and that also call `sched_rr_get_interval()`, were silently corrupted when run on 64-bit systems. ([BZ#557684](https://bugzilla.redhat.com/show_bug.cgi?id=557684)<sup>583</sup>)
- \* the RHTSA-2010:0019 update introduced a regression, preventing WoL from working for network devices using the e1000e driver. ([BZ#559335](https://bugzilla.redhat.com/show_bug.cgi?id=559335)<sup>584</sup>)
- \* adding a bonding interface in mode `balance-alb` to a bridge was not functional. ([BZ#560588](https://bugzilla.redhat.com/show_bug.cgi?id=560588)<sup>585</sup>)
- \* some KVM (Kernel-based Virtual Machine) guests experienced slow performance (and possibly a crash) after suspend/resume. ([BZ#560640](https://bugzilla.redhat.com/show_bug.cgi?id=560640)<sup>586</sup>)

---

<sup>575</sup> <https://www.redhat.com/security/data/cve/CVE-2010-0008.html>

<sup>576</sup> <https://www.redhat.com/security/data/cve/CVE-2010-0415.html>

<sup>577</sup> <https://www.redhat.com/security/data/cve/CVE-2010-0437.html>

<sup>578</sup> <https://www.redhat.com/security/data/cve/CVE-2009-4308.html>

<sup>579</sup> <https://www.redhat.com/security/data/cve/CVE-2010-0003.html>

<sup>580</sup> <https://www.redhat.com/security/data/cve/CVE-2010-0007.html>

<sup>581</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=543449](https://bugzilla.redhat.com/show_bug.cgi?id=543449)

<sup>582</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=553132](https://bugzilla.redhat.com/show_bug.cgi?id=553132)

<sup>583</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=557684](https://bugzilla.redhat.com/show_bug.cgi?id=557684)

<sup>584</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=559335](https://bugzilla.redhat.com/show_bug.cgi?id=559335)

<sup>585</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=560588](https://bugzilla.redhat.com/show_bug.cgi?id=560588)

<sup>586</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=560640](https://bugzilla.redhat.com/show_bug.cgi?id=560640)

- \* on some systems, VF cannot be enabled in dom0. ([BZ#560665](#)<sup>587</sup>)
- \* on systems with certain network cards, a system crash occurred after enabling GRO. ([BZ#561417](#)<sup>588</sup>)
- \* for x86 KVM guests with pvclock enabled, the boot clocks were registered twice, possibly causing KVM to write data to a random memory area during the guest's life. ([BZ#561454](#)<sup>589</sup>)
- \* serious performance degradation for 32-bit applications, that map (mmap) thousands of small files, when run on a 64-bit system. ([BZ#562746](#)<sup>590</sup>)
- \* improved kexec/kdump handling. Previously, on some systems under heavy load, kexec/kdump was not functional. ([BZ#562772](#)<sup>591</sup>)
- \* dom0 was unable to boot when using the Xen hypervisor on a system with a large number of logical CPUs. ([BZ#562777](#)<sup>592</sup>)
- \* a fix for a bug that could potentially cause file system corruption. ([BZ#564281](#)<sup>593</sup>)
- \* a bug caused infrequent cluster issues for users of GFS2. ([BZ#564288](#)<sup>594</sup>)
- \* gfs2\_delete\_inode failed on read-only file systems. ([BZ#564290](#)<sup>595</sup>)

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

## 1.88.2. RHSA-2010:0046: Important security and bug fix update



### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2010:0046](#)<sup>596</sup>

Updated kernel packages that fix multiple security issues and several bugs are now available for Red Hat Enterprise Linux 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security fixes:

- \* an array index error was found in the gdt driver. A local user could send a specially-crafted IOCTL request that would cause a denial of service or, possibly, privilege escalation. ([CVE-2009-3080](#)<sup>597</sup>, Important)

<sup>587</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=560665](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=560665)

<sup>588</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=561417](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=561417)

<sup>589</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=561454](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=561454)

<sup>590</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=562746](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=562746)

<sup>591</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=562772](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=562772)

<sup>592</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=562777](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=562777)

<sup>593</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=564281](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=564281)

<sup>594</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=564288](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=564288)

<sup>595</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=564290](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=564290)

<sup>597</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3080.html>

\* a flaw was found in the FUSE implementation. When a system is low on memory, `fuse_put_request()` could dereference an invalid pointer, possibly leading to a local denial of service or privilege escalation. ([CVE-2009-4021](https://www.redhat.com/security/data/cve/CVE-2009-4021.html)<sup>598</sup>, Important)

\* Tavis Ormandy discovered a deficiency in the `fasync_helper()` implementation. This could allow a local, unprivileged user to leverage a use-after-free of locked, asynchronous file descriptors to cause a denial of service or privilege escalation. ([CVE-2009-4141](https://www.redhat.com/security/data/cve/CVE-2009-4141.html)<sup>599</sup>, Important)

\* the Parallels Virtuozzo Containers team reported the RHTSA-2009:1243 update introduced two flaws in the routing implementation. If an attacker was able to cause a large enough number of collisions in the routing hash table (via specially-crafted packets) for the emergency route flush to trigger, a deadlock could occur. Secondly, if the kernel routing cache was disabled, an uninitialized pointer would be left behind after a route lookup, leading to a kernel panic. ([CVE-2009-4272](https://www.redhat.com/security/data/cve/CVE-2009-4272.html)<sup>600</sup>, Important)

\* the RHTSA-2009:0225 update introduced a rewrite attack flaw in the `do_coredump()` function. A local attacker able to guess the file name a process is going to dump its core to, prior to the process crashing, could use this flaw to append data to the dumped core file. This issue only affects systems that have `"/proc/sys/fs/suid_dumpable"` set to 2 (the default value is 0). ([CVE-2006-6304](https://www.redhat.com/security/data/cve/CVE-2006-6304.html)<sup>601</sup>, Moderate)

The fix for [CVE-2006-6304](https://www.redhat.com/security/data/cve/CVE-2006-6304.html)<sup>602</sup> changes the expected behavior: With `suid_dumpable` set to 2, the core file will not be recorded if the file already exists. For example, core files will not be overwritten on subsequent crashes of processes whose core files map to the same name.

\* an information leak was found in the Linux kernel. On AMD64 systems, 32-bit processes could access and read certain 64-bit registers by temporarily switching themselves to 64-bit mode. ([CVE-2009-2910](https://www.redhat.com/security/data/cve/CVE-2009-2910.html)<sup>603</sup>, Moderate)

\* the RHBA-2008:0314 update introduced N\_Port ID Virtualization (NPIV) support in the `qla2xxx` driver, resulting in two new `sysfs` pseudo files, `"/sys/class/scsi_host/[a qla2xxx host]/vport_create"` and `"vport_delete"`. These two files were world-writable by default, allowing a local user to change SCSI host attributes. This flaw only affects systems using the `qla2xxx` driver and NPIV capable hardware. ([CVE-2009-3556](https://www.redhat.com/security/data/cve/CVE-2009-3556.html)<sup>604</sup>, Moderate)

\* permission issues were found in the `megaraid_sas` driver. The `"dbg_lvl"` and `"poll_mode_io"` files on the `sysfs` file system (`"/sys/"`) had world-writable permissions. This could allow local, unprivileged users to change the behavior of the driver. ([CVE-2009-3889](https://www.redhat.com/security/data/cve/CVE-2009-3889.html)<sup>605</sup>, [CVE-2009-3939](https://www.redhat.com/security/data/cve/CVE-2009-3939.html)<sup>606</sup>, Moderate)

\* a NULL pointer dereference flaw was found in the `firewire-ohci` driver used for OHCI compliant IEEE 1394 controllers. A local, unprivileged user with access to `/dev/fw*` files could issue certain IOCTL calls, causing a denial of service or privilege escalation. The FireWire modules are blacklisted by default, and if enabled, only root has access to the files noted above by default. ([CVE-2009-4138](https://www.redhat.com/security/data/cve/CVE-2009-4138.html)<sup>607</sup>, Moderate)

---

<sup>598</sup> <https://www.redhat.com/security/data/cve/CVE-2009-4021.html>

<sup>599</sup> <https://www.redhat.com/security/data/cve/CVE-2009-4141.html>

<sup>600</sup> <https://www.redhat.com/security/data/cve/CVE-2009-4272.html>

<sup>601</sup> <https://www.redhat.com/security/data/cve/CVE-2006-6304.html>

<sup>602</sup> <https://www.redhat.com/security/data/cve/CVE-2006-6304.html>

<sup>603</sup> <https://www.redhat.com/security/data/cve/CVE-2009-2910.html>

<sup>604</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3556.html>

<sup>605</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3889.html>

<sup>606</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3939.html>

<sup>607</sup> <https://www.redhat.com/security/data/cve/CVE-2009-4138.html>

\* a buffer overflow flaw was found in the `hfs_bnode_read()` function in the HFS file system implementation. This could lead to a denial of service if a user browsed a specially-crafted HFS file system, for example, by running "ls". ([CVE-2009-4020](#)<sup>608</sup>, Low)

Bug fix documentation for this update will be available shortly from [www.redhat.com/docs/en-US/errata/RHSA-2010-0046/Kernel\\_Security\\_Update/index.html](http://www.redhat.com/docs/en-US/errata/RHSA-2010-0046/Kernel_Security_Update/index.html)

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

### 1.88.3. RHSAs-2010:0019: Important security update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2010:0019](#)<sup>609</sup>

Updated kernel packages that fix multiple security issues are now available for Red Hat Enterprise Linux 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

This update fixes the following security issues:

\* a flaw was found in the IPv6 Extension Header (EH) handling implementation in the Linux kernel. The `skb->dst` data structure was not properly validated in the `ipv6_hop_jumbo()` function. This could possibly lead to a remote denial of service. ([CVE-2007-4567](#)<sup>610</sup>, Important)

\* a flaw was found in each of the following Intel PRO/1000 Linux drivers in the Linux kernel: `e1000` and `e1000e`. A remote attacker using packets larger than the MTU could bypass the existing fragment check, resulting in partial, invalid frames being passed to the network stack. These flaws could also possibly be used to trigger a remote denial of service. ([CVE-2009-4536](#)<sup>611</sup>, [CVE-2009-4538](#)<sup>612</sup>, Important)

\* a flaw was found in the Realtek `r8169` Ethernet driver in the Linux kernel. Receiving overly-long frames with network cards supported by this driver could possibly result in a remote denial of service. ([CVE-2009-4537](#)<sup>613</sup>, Important)

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

<sup>608</sup> <https://www.redhat.com/security/data/cve/CVE-2009-4020.html>

<sup>610</sup> <https://www.redhat.com/security/data/cve/CVE-2007-4567.html>

<sup>611</sup> <https://www.redhat.com/security/data/cve/CVE-2009-4536.html>

<sup>612</sup> <https://www.redhat.com/security/data/cve/CVE-2009-4538.html>

<sup>613</sup> <https://www.redhat.com/security/data/cve/CVE-2009-4537.html>



## 1.88.4. RHSA-2009:1670: Important security and bug fix update



### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2009:1670](#)<sup>614</sup>

Updated kernel packages that fix multiple security issues and several bugs are now available for Red Hat Enterprise Linux 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security fixes:

\* NULL pointer dereference flaws in the r128 driver. Checks to test if the Concurrent Command Engine state was initialized were missing in private IOCTL functions. An attacker could use these flaws to cause a local denial of service or escalate their privileges. ([CVE-2009-3620](#)<sup>615</sup>, Important)

\* a NULL pointer dereference flaw in the NFSv4 implementation. Several NFSv4 file locking functions failed to check whether a file had been opened on the server before performing locking operations on it. A local user on a system with an NFSv4 share mounted could possibly use this flaw to cause a denial of service or escalate their privileges. ([CVE-2009-3726](#)<sup>616</sup>, Important)

\* a flaw in `tcf_fill_node()`. A certain data structure in this function was not initialized properly before being copied to user-space. This could lead to an information leak. ([CVE-2009-3612](#)<sup>617</sup>, Moderate)

\* `unix_stream_connect()` did not check if a UNIX domain socket was in the shutdown state. This could lead to a deadlock. A local, unprivileged user could use this flaw to cause a denial of service. ([CVE-2009-3621](#)<sup>618</sup>, Moderate)

Knowledgebase DOC-20536 has steps to mitigate NULL pointer dereference flaws.

Bug fixes:

\* frequently changing a CPU between online and offline caused a kernel panic on some systems. ([BZ#545583](#)<sup>619</sup>)

\* for the LSI Logic LSI53C1030 Ultra320 SCSI controller, read commands sent could receive incorrect data, preventing correct data transfer. ([BZ#529308](#)<sup>620</sup>)

\* `pciehpc` could not detect PCI Express hot plug slots on some systems. ([BZ#530383](#)<sup>621</sup>)

\* soft lockups: inotify race and contention on `dcache_lock`. ([BZ#533822](#)<sup>622</sup>,

[BZ#537019](#)<sup>623</sup>)

---

<sup>615</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3620.html>

<sup>616</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3726.html>

<sup>617</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3612.html>

<sup>618</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3621.html>

<sup>619</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=545583](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=545583)

<sup>620</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=529308](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=529308)

<sup>621</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=530383](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=530383)

<sup>622</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=533822](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=533822)

<sup>623</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=537019](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=537019)



- \* priority ordered lists are now used for threads waiting for a given mutex. ([BZ#533858](#)<sup>624</sup>)
- \* a deadlock in DLM could cause GFS2 file systems to lock up. ([BZ#533859](#)<sup>625</sup>)
- \* use-after-free bug in the audit subsystem crashed certain systems when running usermod. ([BZ#533861](#)<sup>626</sup>)
- \* on certain hardware configurations, a kernel panic when the Broadcom iSCSI offload driver (bnx2i.ko and cnic.ko) was loaded. ([BZ#537014](#)<sup>627</sup>)
- \* qla2xxx: Enabled MSI-X, and correctly handle the module parameter to control it. This improves performance for certain systems. ([BZ#537020](#)<sup>628</sup>)
- \* system crash when reading the cpuaffinity file on a system. ([BZ#537346](#)<sup>629</sup>)
- \* suspend-resume problems on systems with lots of logical CPUs, e.g. BX-EX. ([BZ#539674](#)<sup>630</sup>)
- \* off-by-one error in the legacy PCI bus check. ([BZ#539675](#)<sup>631</sup>)
- \* TSC was not made available on systems with multi-clustered APICs. This could cause slow performance for time-sensitive applications. ([BZ#539676](#)<sup>632</sup>)
- \* ACPI: ARB\_DISABLE now disabled on platforms that do not need it. ([BZ#539677](#)<sup>633</sup>)
- \* fix node to core and power-aware scheduling issues, and a kernel panic during boot on certain AMD Opteron processors. ([BZ#539678](#)<sup>634</sup>, [BZ#540469](#)<sup>635</sup>, [BZ#539680](#)<sup>636</sup>, [BZ#539682](#)<sup>637</sup>)
- \* APIC timer interrupt issues on some AMD Opteron systems prevented achieving full power savings. ([BZ#539681](#)<sup>638</sup>)
- \* general OProfile support for some newer Intel processors. ([BZ#539683](#)<sup>639</sup>)
- \* system crash during boot when NUMA is enabled on systems using MC and kernel-xen. ([BZ#539684](#)<sup>640</sup>)
- \* on some larger systems, performance issues due to a spinlock. ([BZ#539685](#)<sup>641</sup>)
- \* APIC errors when IOMMU is enabled on some AMD Opteron systems. ([BZ#539687](#)<sup>642</sup>)

---

<sup>624</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=533858](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=533858)

<sup>625</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=533859](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=533859)

<sup>626</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=533861](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=533861)

<sup>627</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=537014](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=537014)

<sup>628</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=537020](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=537020)

<sup>629</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=537346](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=537346)

<sup>630</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=539674](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=539674)

<sup>631</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=539675](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=539675)

<sup>632</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=539676](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=539676)

<sup>633</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=539677](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=539677)

<sup>634</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=539678](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=539678)

<sup>635</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=540469](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=540469)

<sup>636</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=539680](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=539680)

<sup>637</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=539682](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=539682)

<sup>638</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=539681](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=539681)

<sup>639</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=539683](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=539683)

<sup>640</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=539684](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=539684)

<sup>641</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=539685](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=539685)

<sup>642</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=539687](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=539687)

\* on some AMD Opteron systems, repeatedly taking a CPU offline then online caused a system hang. ([BZ#539688](#)<sup>643</sup>)

\* I/O page fault errors on some systems. ([BZ#539689](#)<sup>644</sup>)

\* certain memory configurations could cause the kernel-xen kernel to fail to boot on some AMD Opteron systems. ([BZ#539690](#)<sup>645</sup>)

\* NMI watchdog is now disabled for offline CPUs. ([BZ#539691](#)<sup>646</sup>)

\* duplicate directories in /proc/acpi/processor/ on BX-EX systems. ([BZ#539692](#)<sup>647</sup>)

\* links did not come up when using bnx2x with certain Broadcom devices. ([BZ#540381](#)<sup>648</sup>)

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

### 1.88.5. RHSA-2009:1548: Important security and bug fix update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2009:1548](#)<sup>649</sup>

Updated kernel packages that fix multiple security issues and several bugs are now available for Red Hat Enterprise Linux 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security fixes:

\* a system with SELinux enforced was more permissive in allowing local users in the unconfined\_t domain to map low memory areas even if the mmap\_min\_addr restriction was enabled. This could aid in the local exploitation of NULL pointer dereference bugs. ([CVE-2009-2695](#)<sup>650</sup>, Important)

\* a NULL pointer dereference flaw was found in the eCryptfs implementation in the Linux kernel. A local attacker could use this flaw to cause a local denial of service or escalate their privileges. ([CVE-2009-2908](#)<sup>651</sup>, Important)

\* a flaw was found in the NFSv4 implementation. The kernel would do an unnecessary permission check after creating a file. This check would usually fail and leave the file with the permission bits set to random values. Note: This is a server-side only issue. ([CVE-2009-3286](#)<sup>652</sup>, Important)

---

<sup>643</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=539688](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=539688)

<sup>644</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=539689](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=539689)

<sup>645</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=539690](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=539690)

<sup>646</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=539691](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=539691)

<sup>647</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=539692](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=539692)

<sup>648</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=540381](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=540381)

<sup>650</sup> <https://www.redhat.com/security/data/cve/CVE-2009-2695.html>

<sup>651</sup> <https://www.redhat.com/security/data/cve/CVE-2009-2908.html>

<sup>652</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3286.html>

\* a NULL pointer dereference flaw was found in each of the following functions in the Linux kernel: pipe\_read\_open(), pipe\_write\_open(), and pipe\_rdwr\_open(). When the mutex lock is not held, the i\_pipe pointer could be released by other processes before it is used to update the pipe's reader and writer counters. This could lead to a local denial of service or privilege escalation. ([CVE-2009-3547](https://www.redhat.com/security/data/cve/CVE-2009-3547.html)<sup>653</sup>, Important)

\* a flaw was found in the Realtek r8169 Ethernet driver in the Linux kernel. pci\_unmap\_single() presented a memory leak that could lead to IOMMU space exhaustion and a system crash. An attacker on the local network could abuse this flaw by using jumbo frames for large amounts of network traffic. ([CVE-2009-3613](https://www.redhat.com/security/data/cve/CVE-2009-3613.html)<sup>654</sup>, Important)

\* missing initialization flaws were found in the Linux kernel. Padding data in several core network structures was not initialized properly before being sent to user-space. These flaws could lead to information leaks. ([CVE-2009-3228](https://www.redhat.com/security/data/cve/CVE-2009-3228.html)<sup>655</sup>, Moderate)

#### Bug fixes:

\* with network bonding in the "balance-tlb" or "balance-alb" mode, the primary setting for the primary slave device was lost when said device was brought down. Bringing the slave back up did not restore the primary setting. ([BZ#517971](https://bugzilla.redhat.com/show_bug.cgi?id=517971)<sup>656</sup>)

\* some faulty serial device hardware caused systems running the kernel-xen kernel to take a very long time to boot. ([BZ#524153](https://bugzilla.redhat.com/show_bug.cgi?id=524153)<sup>657</sup>)

\* a caching bug in nfs\_readdir() may have caused NFS clients to see duplicate files or not see all files in a directory. ([BZ#526960](https://bugzilla.redhat.com/show_bug.cgi?id=526960)<sup>658</sup>)

\* the RHSA-2009:1243 update removed the mpt\_msi\_enable option, preventing certain scripts from running. This update adds the option back. ([BZ#526963](https://bugzilla.redhat.com/show_bug.cgi?id=526963)<sup>659</sup>)

\* an iptables rule with the recent module and a hit count value greater than the ip\_pkt\_list\_tot parameter (the default is 20), did not have any effect over packets, as the hit count could not be reached. ([BZ#527434](https://bugzilla.redhat.com/show_bug.cgi?id=527434)<sup>660</sup>)

\* a check has been added to the IPv4 code to make sure that rt is not NULL, to help prevent future bugs in functions that call ip\_append\_data() from being exploitable. ([BZ#527436](https://bugzilla.redhat.com/show_bug.cgi?id=527436)<sup>661</sup>)

\* a kernel panic occurred in certain conditions after reconfiguring a tape drive's block size. ([BZ#528133](https://bugzilla.redhat.com/show_bug.cgi?id=528133)<sup>662</sup>)

\* when using the Linux Virtual Server (LVS) in a master and backup configuration, and propagating active connections on the master to the backup, the connection timeout value on the backup was hard-coded to 180 seconds, meaning connection information on the backup was soon lost. This could prevent the successful failover of connections. The timeout value can now be set via "ipvsadm --set". ([BZ#528645](https://bugzilla.redhat.com/show_bug.cgi?id=528645)<sup>663</sup>)

<sup>653</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3547.html>

<sup>654</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3613.html>

<sup>655</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3228.html>

<sup>656</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=517971](https://bugzilla.redhat.com/show_bug.cgi?id=517971)

<sup>657</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=524153](https://bugzilla.redhat.com/show_bug.cgi?id=524153)

<sup>658</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=526960](https://bugzilla.redhat.com/show_bug.cgi?id=526960)

<sup>659</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=526963](https://bugzilla.redhat.com/show_bug.cgi?id=526963)

<sup>660</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=527434](https://bugzilla.redhat.com/show_bug.cgi?id=527434)

<sup>661</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=527436](https://bugzilla.redhat.com/show_bug.cgi?id=527436)

<sup>662</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=528133](https://bugzilla.redhat.com/show_bug.cgi?id=528133)

<sup>663</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=528645](https://bugzilla.redhat.com/show_bug.cgi?id=528645)

\* a bug in `nfs4_do_open_expired()` could have caused the reclaimer thread on an NFSv4 client to enter an infinite loop. ([BZ#529162](#)<sup>664</sup>)

\* MSI interrupts may not have been delivered for r8169 based network cards that have MSI interrupts enabled. This bug only affected certain systems. ([BZ#529366](#)<sup>665</sup>)

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

### 1.88.6. RHSA-2009:1455: Moderate security and bug fix update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2009:1455](#)<sup>666</sup>

Updated kernel packages that fix one security issue and several bugs are now available for Red Hat Enterprise Linux 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

[Updated 23rd February 2010] This update adds references to two KBase articles that includes greater detail regarding some bug fixes that could not be fully documented in the errata note properly.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security fix:

\* a NULL pointer dereference flaw was found in the Multiple Devices (md) driver in the Linux kernel. If the "suspend\_lo" or "suspend\_hi" file on the sysfs file system ("/sys/") is modified when the disk array is inactive, it could lead to a local denial of service or privilege escalation. Note: By default, only the root user can write to the files noted above. ([CVE-2009-2849](#)<sup>667</sup>, Moderate)

Bug fixes:

\* a bug in `nlm_lookup_host()` could lead to un-reclaimed file system locks, resulting in amount failing & NFS service relocation issues for clusters. ([BZ#517967](#)<sup>668</sup>)

\* a bug in the sky2 driver prevented the phy from being reset properly on some hardware when it hung, preventing a link from coming back up. ([BZ#517976](#)<sup>669</sup>)

\* disabling MSI-X for qla2xxx also disabled MSI interrupts. ([BZ#519782](#)<sup>671</sup><sup>670</sup>)

\* performance issues with reads when using the qlge driver on PowerPC systems. A system hang could also occur during reboot. ([BZ#519783](#)<sup>672</sup>)

---

<sup>664</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=529162](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=529162)

<sup>665</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=529366](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=529366)

<sup>667</sup> <https://www.redhat.com/security/data/cve/CVE-2009-2849.html>

<sup>668</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=517967](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=517967)

<sup>669</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=517976](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=517976)

<sup>671</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=519782](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=519782)

<sup>670</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=519782](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=519782)

<sup>672</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=519783](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=519783)

- \* unreliable time keeping for Red Hat Enterprise Linux virtual machines. The KVM pvclock code is now used to detect/correct lost ticks. ([BZ#520685](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=520685)<sup>673</sup>)
- \* /proc/cpuinfo was missing flags for new features in supported processors, possibly preventing the operating system & applications from getting the best performance. ([BZ#520686](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=520686)<sup>674</sup>)
- \* reading/writing with a serial loopback device on a certain IBM system did not work unless booted with "pnpacpi=off". ([BZ#520905](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=520905)<sup>675</sup>)
- \* mlx4\_core failed to load on systems with more than 32 CPUs. ([BZ#520906](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=520906)<sup>677676</sup>)
- \* on big-endian platforms, interfaces using the mlx4\_en driver & Large Receive Offload (LRO) did not handle VLAN traffic properly (a segmentation fault in the VLAN stack in the kernel occurred). ([BZ#520908](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=520908)<sup>678</sup>)
- \* due to a lock being held for a long time, some systems may have experienced "BUG: soft lockup" messages under heavy load. ([BZ#520919](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=520919)<sup>679</sup>)
- \* incorrect APIC timer calibration may have caused a system hang during boot, as well as the system time becoming faster or slower. A warning is now provided. ([BZ#521238](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=521238)<sup>680</sup>)
- \* a Fibre Channel device re-scan via 'echo "---" > /sys/class/scsi\_host/ host[x]/scan' may not complete after hot adding a drive, leading to soft lockups ("BUG: soft lockup detected"). ([BZ#521239](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=521239)<sup>681</sup>)
- \* the Broadcom BCM5761 network device could not be initialized properly; therefore, the associated interface could not obtain an IP address via DHCP or be assigned one manually. ([BZ#521241](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=521241)<sup>682</sup>)
- \* when a process attempted to read from a page that had first been accessed by writing to part of it (via write(2)), the NFS client needed to flush the modified portion of the page out to the server, & then read the entire page back in. This flush caused performance issues. ([BZ#521244](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=521244)<sup>683</sup>)
- \* a kernel panic when using bnx2x devices & LRO in a bridge. A warning is now provided to disable LRO in these situations. ([BZ#522636](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=522636)<sup>684</sup>)
- \* the scsi\_dh\_rdac driver was updated to recognize the Sun StorageTek Flexline 380. ([BZ#523237](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=523237)<sup>685</sup>)
- \* in FIPS mode, random number generators are required to not return the first block of random data they generate, but rather save it to seed the repetition check. This update brings the random number generator into conformance. ([BZ#523289](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=523289)<sup>686</sup>)
- \* an option to disable/enable the use of the first random block is now provided to bring ansi\_cprng into compliance with FIPS-140 continuous test requirements. ([BZ#523290](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=523290)<sup>687</sup>)

<sup>673</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=520685](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=520685)

<sup>674</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=520686](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=520686)

<sup>675</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=520905](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=520905)

<sup>677</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=520906](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=520906)

<sup>676</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=520906](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=520906)

<sup>678</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=520908](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=520908)

<sup>679</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=520919](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=520919)

<sup>680</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=521238](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=521238)

<sup>681</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=521239](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=521239)

<sup>682</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=521241](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=521241)

<sup>683</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=521244](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=521244)

<sup>684</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=522636](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=522636)

<sup>685</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=523237](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=523237)

<sup>686</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=523289](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=523289)

<sup>687</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=523290](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=523290)

\* running the SAP Linux Certification Suite in a KVM guest caused severe SAP kernel errors, causing it to exit. ([BZ#524150](#)<sup>688</sup>)

\* attempting to 'online' a CPU for a KVM guest via sysfs caused a system crash. ([BZ#524151](#)<sup>689</sup>)

\* when using KVM, pvclock returned bogus wallclock values. ([BZ#524152](#)<sup>690</sup>)

\* the clock could go backwards when using the vsyscall infrastructure. ([BZ#524527](#)<sup>691</sup>)

See References for KBase links re [BZ#519782](#)<sup>693692</sup> & [BZ#520906](#)<sup>695694</sup>.

Users should upgrade to these updated packages, which contain backported patches to correct these issues. Reboot the system for this update to take effect.

### 1.88.7. RHSA-2010:0178: Important Red Hat Enterprise Linux 5.5 kernel security and bug fix update

Updated kernel packages that fix three security issues, address several hundred bugs, and add numerous enhancements are now available as part of the ongoing support and maintenance of Red Hat Enterprise Linux version 5. This is the fifth regular update.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

This update fixes the following security issues:

\* a race condition was found in the mac80211 implementation, a framework used for writing drivers for wireless devices. An attacker could trigger this flaw by sending a Delete Block ACK (DELBA) packet to a target system, resulting in a remote denial of service. Note: This issue only affected users on 802.11n networks, and that also use the iwlnagn driver with Intel wireless hardware. ([CVE-2009-4027](#)<sup>696</sup>, Important)

\* a flaw was found in the gfs2\_lock() implementation. The GFS2 locking code could skip the lock operation for files that have the S\_ISGID bit (set-group-ID on execution) in their mode set. A local, unprivileged user on a system that has a GFS2 file system mounted could use this flaw to cause a kernel panic. ([CVE-2010-0727](#)<sup>697</sup>, Moderate)

\* a divide-by-zero flaw was found in the ext4 file system code. A local attacker could use this flaw to cause a denial of service by mounting a specially-crafted ext4 file system. ([CVE-2009-4307](#)<sup>698</sup>, Low)

These updated packages also include several hundred bug fixes for and enhancements to the Linux kernel. Space precludes documenting each of these changes in this advisory and users are directed

---

<sup>688</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=524150](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=524150)

<sup>689</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=524151](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=524151)

<sup>690</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=524152](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=524152)

<sup>691</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=524527](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=524527)

<sup>693</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=519782](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=519782)

<sup>692</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=519782](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=519782)

<sup>695</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=520906](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=520906)

<sup>694</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=520906](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=520906)

<sup>696</sup> <https://www.redhat.com/security/data/cve/CVE-2009-4027.html>

<sup>697</sup> <https://www.redhat.com/security/data/cve/CVE-2010-0727.html>

<sup>698</sup> <https://www.redhat.com/security/data/cve/CVE-2009-4307.html>



to the Red Hat Enterprise Linux 5.5 Release Notes for information on the most significant of these changes:

[http://www.redhat.com/docs/en-US/Red\\_Hat\\_Enterprise\\_Linux/5.5/html/Release\\_Notes/](http://www.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/5.5/html/Release_Notes/)

All Red Hat Enterprise Linux 5 users are advised to install these updated packages, which address these vulnerabilities as well as fixing the bugs and adding the enhancements noted in the Red Hat Enterprise Linux 5.5 Release Notes and Technical Notes. The system must be rebooted for this update to take effect.

### 1.88.7.1. Bug Fixes

The following is a list of the bugs that have been addressed in this kernel release, including causes, consequences, and fix results.

#### 1.88.7.1.1. Generic Kernel Features

- Add IRONLAKE support to AGP/DRM drivers. [BZ#547908](#)<sup>699</sup>
- PCI AER: HEST FIRMWARE FIRST support. [BZ#547762](#)<sup>700</sup>
- Extend tracepoint support. [BZ#534178](#)<sup>701</sup>
- Update ibmvscsi driver with upstream multipath enhancements. [BZ#512203](#)<sup>702</sup>

This update provides improved support for the ibmvscsi driver, including support for fastfail mode and improved multipathing support.

This update is 64-bit PowerPC-specific.

- amd64\_edac: Add and detect ddr3 support. [BZ#479070](#)<sup>703</sup>
- Add scsi and libfc symbols to whitelist\_file. [BZ#533489](#)<sup>704</sup>
- Extend KABI to support symbols that are not part of the current KABI. [BZ#526342](#)<sup>705</sup>
- libfc bug fixes and improvements. [BZ#526259](#)<sup>706</sup>
- Implement smp\_call\_function\_[single|many] in x86\_64 and i386. [BZ#526043](#)<sup>707</sup>

A number of updates now depend on the smp\_call\_function\_single() and smp\_call\_function\_many() functions. This update provides a single function that can refer to the appropriate function as required, thereby simplifying the creation of further updates.

- Support the single-port Async device on p7 Saturn. [BZ#525812](#)<sup>708</sup>
- Backport open source driver for Creative X-Fi audio card. [BZ#523786](#)<sup>709</sup>
- [Intel 5.5 FEAT] Update PCI.IDS for B43 graphics controller. [BZ#523637](#)<sup>710</sup>
- Support physical CPU hotplug. [BZ#516999](#)<sup>711</sup>

This feature provides the functionality to add and remove CPU resources physically while the system is running.

This feature applies to 32-bit x86, 64-bit Intel 64 and AMD64, and 64-bit Itanium2 architectures.

- Include core WMI support and Dell-WMI driver. [BZ#516623](#)<sup>712</sup>
- [kabi] Add `scsi_nl_{send_vendor_msg,{add,remove}_driver}`. [BZ#515812](#)<sup>713</sup>
- Enable ACPI 4.0 power metering. [BZ#514923](#)<sup>714</sup>
- Add AER software error injection support. [BZ#514442](#)<sup>715</sup>
- Add support for Syleus chip to `fschmd` driver. [BZ#513101](#)<sup>716</sup>
- Implement support for DS8000 volumes. [BZ#511972](#)<sup>717</sup>
- Support Lexar ExpressCard. [BZ#511374](#)<sup>718</sup>
- Disable `ARB_DISABLE` on platforms where it is not needed. [BZ#509422](#)<sup>719</sup>

`ARB_DISABLE` is a NOP on all of the recent Intel platforms. For such platforms, this update reduces contention on the `c3_lock` by skipping the fake `ARB_DISABLE`.

This lock is held on each deep C-state entry and exit and with 16, 32, and 64 logical CPUs in NHM EP, NHM EX platforms, this contention can become significant. Specifically on distributions that do not have tickless feature and where all CPUs may wake up around the same time.

- Add `zfc` parameter to dynamically adjust `scsi_queue_depth` size. [BZ#508355](#)<sup>720</sup>
- Add HP ipmi message handling to Red Hat Enterprise Linux 5. [BZ#507402](#)<sup>721</sup>
- Backport `CONFIG_DETECT_HUNG_TASK` to Red Hat Enterprise Linux 5. [BZ#506059](#)<sup>722</sup>

In some circumstances, tasks in the kernel may permanently enter the uninterruptible sleep state (D-State), making the system impossible to shut down. This update adds the Detect Hung Task kernel thread, providing the ability to detect tasks permanently stuck in the D-State.

This new feature is controlled by the "`CONFIG_DETECT_HUNG_TASK=`" kernel flag. When set to "y", tasks stuck in the D-State are detected; when set to "n" it is off. The default value for the "`CONFIG_DETECT_HUNG_TASK`" flag is "y".

Additionally, the "`CONFIG_BOOTPARAM_HUNG_TASK_PANIC`" flag has been added. When set to "y", a kernel panic is triggered when a task stuck in the D-State is detected. The default value for the "`CONFIG_BOOTPARAM_HUNG_TASK_PANIC`" flag is "n".

- Add ability to access Nehalem uncore configuration space. [BZ#504330](#)<sup>723</sup>

Systems that don't use `MMCONFIG` have trouble when allocating resources by using a legacy PCI probe. As a result, the machine will hang during boot if the Disk PCI device is not properly initialized.

This update reverts a patch that improves the PCI ID detection in order to detect the new PCI devices found on Nehalem machines. Consequently, the kernel will not hang on such machines. A different patch will be needed, however, when adding any driver that needs to see the non-core set of PCI devices on Nehalem.

- When booted with P-state limit, limit can never be increased [BZ#489566](#)<sup>724</sup>
- Add `do_settimeofday` and `__user_walk_fd` [BZ#486205](#)<sup>725</sup>



- A bug was discovered where closing the lid on an HP6510b caused the system to crash. This was due to the system failing to run on CPU0. A patch was created to enable ACPI workqueues to run on CPU0, and this has been tested successfully. [BZ#485016](#)<sup>726</sup>
- Some applications (e.g., dump and nfsd) try to improve disk I/O performance by distributing I/O requests to multiple processes or threads by using the Completely Fair Queuing (CFQ) I/O scheduler. This application design negatively affected I/O performance, causing a large drop in performance under certain workloads on real queuing devices.

The kernel can now detect and merge cooperating queues. Further, it can also detect if the queues stop cooperating, and split them apart again. I/O performance is no longer negatively affected by using the CFQ scheduler. [BZ#427709](#)<sup>727</sup> [BZ#456181](#)<sup>728</sup> [BZ#448130](#)<sup>729</sup>

- Enable CONFIG\_DETECT\_HUNG\_TASK by default, but disable BOOTPARAM\_xx by default
- Only prompt for network configuration when required. [BZ#506898](#)<sup>730</sup>

Due to an unexpected side effect of a kernel change in Red Hat Enterprise Linux 5.4, the installer will prompt for the network configuration, regardless of whether these parameters appear in the PARM or CONF files.

This flaw was addressed by removing the annotation of cmdline as \_\_initdata. The installer no longer prompts for network configuration when not required.

### 1.88.7.1.2. Kernel Platform Enablement

#### 1.88.7.1.2.1. BX-EX/MC Enablement Features

- [Intel 5.5 FEAT] Make suspend-resume work on systems with lots of logical CPUs (Boxboro-EX). [BZ#499271](#)<sup>731</sup>
- [Intel 5.5 FEAT] Add ability to access Nehalem uncore config space 504330/539675
- [AMD 5.5 Feat] Support Magny-cours topology 513684/539678
- Red Hat Enterprise Linux 5.5: Power-aware Scheduler changes to support multiple node processors 513685/539680
- Fix kernel panic while booting Red Hat Enterprise Linux 5 32-bit kernel on Magny-cours. [BZ#522215](#)<sup>732</sup>
- [Intel 5.5 FEAT] Oprofile: Add support for arch perfmon - kernel component [BZ#523479](#)<sup>733</sup>
- EXPERIMENTAL EX/MC: Xen NUMA broken on Magny-cours system Z. [BZ#526051](#)<sup>734</sup>
- [Intel 5.5 FEAT] Fix spinlock issue which causes performance impact on large systems. [BZ#526078](#)<sup>735</sup>
- EXPERIMENTAL EX/MC: Magny-cours topology fixes. [BZ#526315](#)<sup>736</sup>
- EXPERIMENTAL MC/EX: Issue when bringing CPU offline and online with 32-bit kernel. [BZ#526770](#)<sup>737</sup>
- EXPERIMENTAL MC/EX: Incorrect memory setup can cause Xen crash. [BZ#526785](#)<sup>738</sup>

- Fix AMD erratum - server C1E [BZ#519422](#)<sup>739</sup>
- EXPERIMENTAL EX/MC: AMD IOMMU Linux driver with latest BIOS has IO PAGE FAULTS 531469/539689
- [Intel 5.5 BUG] NMI and Watchdog are not disabled on CPU when CPU is taken offline. [BZ#532514](#)<sup>740</sup>
- Boxboro-EX: multiple equal directory entries in `/proc/acpi/processor` [BZ#537395](#)<sup>741</sup>

### 1.88.7.1.2.2. x86-specific Updates

- Fix AMD Magny-Cours boot inside Xen on pre-5.5 hypervisor. [BZ#560013](#)<sup>742</sup>

A problem was found where Beta 1 of Red Hat Enterprise Linux 5.5 would fail to boot as a Xen guest on AMD Magny-Cours systems using a hypervisor other than the one included in Red Hat Enterprise Linux 5.5.

This update provides a fix for this issue.

- Support always running local APIC. [BZ#496306](#)<sup>743</sup>
- kvm: Mark `kvmclock_init` as `cpuinit`. [BZ#523450](#)<sup>744</sup>
- Fix stale data in `shared_cpu_map` `cpumasks`. [BZ#541953](#)<sup>745</sup>

This update was necessary to avoid possible kernel panic when performing frequent CPU online/offline operations.

### 1.88.7.1.2.3. x86\_64-specific Updates

- k8: Do not mark `early_is_k8_nb` as `__init`. [BZ#567275](#)<sup>746</sup>

This update addresses a problem with CPU hotplugging identified on AMD Magny-Cours machines.

- Avoid deadlocks during MCE broadcasts. [BZ#562866](#)<sup>747</sup>
- Wire up compat `sched_rr_get_interval`. [BZ#557092](#)<sup>748</sup>

A problem was found where if a program that calls `sched_rr_get_interval()` is compiled on x86 and is executed on x86\_64, it will destroy the user stack. This problem is solved by calling `sys32_sched_rr_get_interval()` instead of `sys_sched_rr_get_interval()` when `sched_rr_get_interval()` is called.

This update includes a backport of an upstream patch to correct this problem.

- Disable `vsyscall` in kvm guests. [BZ#542612](#)<sup>749</sup>

A problem was found on Red Hat Enterprise Linux 5.4 guests with PV clock enabled, where there is a large difference between the time returned by `clock_gettime(CLOCK_REALTIME)` and the time returned by `gettimeofday()`, even if a program executes one call right after the other.

This update addresses the problem, which was traced to the use of `vsyscall` in kvm guests.

- Resolve issue with SCTP messages arriving out of order. [BZ#517504](#)<sup>750</sup>

A problem was found where, under the right conditions, it was possible for packets to become re-ordered prior to the assignment of a Transmission Sequence Number (TSN) value. The conditions which caused this are the fact that multiple interfaces were used in transmission, where each had differing Path Maximum Transmission Unit (pmtu) values.

This update addresses the problem with the SCTP stack that allowed this reordering to occur.

- Cap kernel at 1024G on x86\_64 systems.
- Fix kernel crash when 1TB of memory and NUMA is used. [BZ#523522](#)<sup>751</sup>
- kvm: Allow kvmclock to be overwritten. [BZ#523447](#)<sup>752</sup>
- glibc should call pselect() and ppoll() on Itanium kernels. [BZ#520867](#)<sup>753</sup>
- Force Altix drivers to use 64-bit addressing. This update is Altix-specific. [BZ#517192](#)<sup>754</sup>

This update applies to the 64-bit Itanium2 architecture.

- vsmp: Fix bit-wise operator and compile issue. [BZ#515408](#)<sup>755</sup>
- Fix hugepage memory tracking. [BZ#518671](#)<sup>756</sup>

#### 1.88.7.1.2.4. IBM S/390-specific Updates

- qeth: Set default BLKT settings by OSA hw level. [BZ#559621](#)<sup>757</sup>

A problem was found where new hardware was being configured with values for old hw levels, because BLKT settings were not being set according to different hw levels.

This update ensures that the BLKT settings are applied after the hw level has been probed.

- Clear high-order bits after switching to 64-bit mode. [BZ#546302](#)<sup>758</sup>
- Fix single stepping on svc 0. [BZ#540527](#)<sup>759</sup>

A problem was found where if a system call number > 256 is single-stepped or svc 0 is single-stepped then the system call would not be executed. This update provides a solution to this problem.

- DASD: Support DIAG access for read-only devices. [BZ#537859](#)<sup>760</sup>
- IUCV: Use correct output register in `iucv_query_maxconn()`. [BZ#524251](#)<sup>761</sup>

A problem was found where the system log contained kernel messages reporting that the IUCV "pathid" was greater than `max_connections`. This is because the wrong output register was used when querying the maximum number of IUCV connections.

This update ensures that the correct output register is used, and this problem no longer occurs.

- cio: Fix set online/offline processing failures. [BZ#523323](#)<sup>762</sup>

A problem was found where the `set online` or `set offline` routines failed for a DASD device. Afterwards this device could neither be set online nor offline.

The **set online**, **set offline**, and related rollback and error routines are only processed if the device is in a FINAL or DISCONNECTED state.

- DASD: Fail requests when device state is less than ready. [BZ#523219](#)<sup>763</sup>

A problem was found where in certain device mapper multipath/PPRC setups a DASD device gets quiesced and then set to the "basic" state to flush its queue and return all already queued requests back to the device mapper. It was possible that a request was queued after the device's state was set to basic, and so that request stayed queued, was not processed, and the device mapper was blocked waiting for it.

This update ensures that all requests that arrive in such a state are returned as failed.

- Set preferred IBM S/390 console based on conmode. [BZ#520461](#)<sup>764</sup>

A problem was found where if conmode was set to 3270 to enable the 3270 terminal device driver, kernel console messages were not displayed in the console view. This is because the default preferred console is set to "ttyS". For the 3270 terminal device driver, the preferred console must be set to "tty3270".

This update introduces a new function to set the preferred console based on the specified conmode.

- Optimize storage key operations for anonymous pages. [BZ#519977](#)<sup>765</sup>

A problem was found where removal of anonymous mappings resulted in poor performance. This update optimizes the instructions that are used for these operations.

- CIO: set correct number of internal I/O retries. [BZ#519814](#)<sup>766</sup>

A problem was found where if a device has *n* paths and that device is not path-grouped, and an internal I/O command fails, then the control unit presents the error sense *n* times on each different path. Because CIO only performs five retries, devices with five or more paths run out of retries before their functional status can be correctly determined.

This update increases the number of retries to 10 to prevent this problem from occurring.

- Add module signing to IBM S/390 kernels. [BZ#483665](#)<sup>767</sup>
- Make CIO\_\* macros safe if dbfs are not available. [BZ#508934](#)<sup>768</sup>
- qeth: Improve no\_checksumming handling for layer3. [BZ#503238](#)<sup>769</sup>
- qeth: Handle VSwitch Port Isolation error codes. [BZ#503232](#)<sup>770</sup>
- Implement AF\_IUCV SOCK\_SEQPACKET support. [BZ#512006](#)<sup>771</sup>

This update offers AF\_IUCV datagram stream-oriented sockets in addition to the existing AF\_IUCV byte stream-oriented sockets. SOCK\_SEQPACKET provides a sequenced, reliable, two-way connection-based data transmission path for datagrams of fixed maximum length; a consumer is required to read an entire packet with each input system call.

- Kernel parameters vmhalt, vmpanic, vmpoff and vmreboot are ignored. [BZ#518229](#)<sup>772</sup>

A problem was found where an obsolete function (`__setup()`) was being called twice. This update removes those function calls, and the affected kernel parameters now behave as expected.

### 1.88.7.1.2.5. Other Updates

- [PowerPC] Fix "scheduling while atomic" error in alignment handler. [BZ#543637](#)<sup>773</sup>
- [powerpc] Handle SLB resize during migration. [BZ#524112](#)<sup>774</sup>
- Export additional CPU flags in `/proc/cpuinfo` [BZ#517928](#)<sup>775</sup>

Previously, `/proc/cpuinfo` only showed the original set of flags supported from the base kernel release. It did not include new features present in supported CPUs. This update addresses this problem, and applies to both x86 and x86\_64 architectures.

- This feature provides the ability for user level software monitoring the system for disabled cache indices and to explicitly disable them. [BZ#517586](#)<sup>776</sup>

This update applies to 32-bit x86 and 64-bit Intel 64 and AMD64 architectures.

- Update ALSA HDA, `snd-hda-intel` driver. [BZ#525390](#)<sup>777</sup>
- Add Hudson-2 sb900 i2c driver. [BZ#515125](#)<sup>778</sup>
- Add fcocee npiv support to `ibmvfc` driver. [BZ#512192](#)<sup>779</sup>
- Add i3200 edac driver support. [BZ#469976](#)<sup>780</sup>

### 1.88.7.1.3. Virtualization Updates

- Fix module loading for `virtio-balloon` module. [BZ#564361](#)<sup>781</sup>
- VT-d: Ignore unknown DMAR entries. [BZ#563900](#)<sup>782</sup>
- kvm: Fix double registering of `pvclock` on i386. [BZ#557095](#)<sup>783</sup>
- Fix frequency scaling on Intel platforms. [BZ#553324](#)<sup>784</sup>
- Update to enable VF in Dom0. [BZ#547980](#)<sup>785</sup>
- Xen IOMMU fix for AMD M-C platforms with SATA set to IDE combined mode. [BZ#544021](#)<sup>786</sup>

AMD M-C systems, that is, Maranello platforms, have several SATA settings, for example, IDE, SATA AHCI, and SATA IDE combined mode. A problem was found with IOMMU when the SATA drive is in IDE combined mode that could prevent Red Hat Enterprise Linux 5.4 from booting properly when IOMMU is enabled. In some cases the SATA drive was not detected.

This update implements a global interrupt remapping table, which is shared by all devices and provides better compatibility with certain old BIOSes, and prevents this problem from occurring.

- Ensure a new `xenfb` thread is not created on every save/restore. [BZ#541325](#)<sup>787</sup>

A problem was found where an initial two `xenfb` threads were created for a save/restore operation for a live migration, followed by another two every time the guest was live migrated, or saved and restored.

This update avoids creating further threads if one already exists.

- PV guest crash on poweroff. [BZ#540811](#)<sup>788</sup>

- Call trace error when resuming from suspend to disk. [BZ#539521](#)<sup>789</sup>
- Add BL2xx and DL7xx to the list of ProLiant systems in `xen/arch/x86/ioport_emulate.c` in the Xen variants of Red Hat Enterprise Linux 5. [BZ#536677](#)<sup>790</sup>
- Mask out extended topology CPUID feature. [BZ#533292](#)<sup>791</sup>

On Intel Nehalem (55xx) dom0 hosts, booting Windows 2008 R2 64-bit domU resulted in a hang. This was caused by incomplete emulation of the CPUID instruction in hvm/xvm support.

Because Xen guests do not need to know about extended topology, this update masks out that topology to prevent this problem from occurring.

- Fix timedrift on VM with `pv_clock` enabled. [BZ#531268](#)<sup>792</sup>
- Use upstream `kvm_get_tsc_khz()` [BZ#531025](#)<sup>793</sup>
- Whitespace updates in Xen scheduler. [BZ#529271](#)<sup>794</sup>
- Xen panic in `msi_msg_read_remap_rte` with `acpi=off`. [BZ#525467](#)<sup>795</sup>
- Backport interrupt rate limiting. [BZ#524747](#)<sup>796</sup>
- RHEV: SAP SLCS 2.3 fails during install/import in a RHEV-H/KVM guest with PV KVM clock. [BZ#524076](#)<sup>797</sup>
- Mask out `xsave` and `osxsave` to prevent boot hang when installing HVM DomU. [BZ#524052](#)<sup>798</sup>

Attempting to boot a fully virtualized DomU with rawhide's 2.6.31-14.fc12.x86\_64 for installation hangs almost immediately. A 32-bit HVM booted and installed successfully on a 32-bit host.

This update masks out the `xsave` and `osxsave` bits to prevent this problem from occurring.

- Enable display of the `ida` flag on Xen kernels. [BZ#522846](#)<sup>799</sup>

The `ida` flag, which indicates the presence of the Turbo Boost feature, was not seen in the `cpuinfo` section of `/proc/cpuinfo` on Xen kernels. This occurred on both 32-bit and 64-bit Xen kernels.

This update ensures that this flag is displayed when the Turbo Boost feature is present on Xen kernels.

- Xen fails to boot on Itanium with > 128GB memory. [BZ#521865](#)<sup>800</sup>

A problem was found where attempting to boot a Xen kernel on Itanium systems with more than 128GB of RAM would result in a Xen panic. This problem was traced to a miscalculation of the Xen heap size.

This update includes support for the `xenheap_megabytes` hypervisor option to address this problem. For example, if the installed memory exceeds 64GB, it is suggested to set the option to a value equal to the memory size in gigabytes. For example, on a system with 128GB of memory, the `elilo.conf` file should include the directive: `append="xenheap_megabytes=128 - -"`

- Fix SRAT check for discontinuous memory. [BZ#519225](#)<sup>801</sup>

A problem was found where Xen could ignore valid SRAT tables because it expects completely contiguous memory ranges, where the sum of the node memory is approximately equal to the

address of the highest memory page. This is an incorrect assumption and prevents NUMA support from being enabled on some systems. This update addresses this assumption and prevents this problem from occurring.

- Allow booting with broken serial hardware. [BZ#518338](#)<sup>802</sup>
- Fix for array out-of-bounds in blkfront. [BZ#517238](#)<sup>803</sup>
- Enable Xen to build on gcc 4.4. [BZ#510686](#)<sup>804</sup>
- Handle x87 opcodes in TLS segment fixup. [BZ#510225](#)<sup>805</sup>
- Implement fully preemptible page table teardown. [BZ#510037](#)<sup>806</sup>
- Fix timeout with PV guest and physical CDROM. [BZ#506899](#)<sup>807</sup>
- Fix SR-IOV function dependency link problem. [BZ#503837](#)<sup>808</sup>
- F-11 Xen 64-bit domU cannot be started with > 2047MB of memory. [BZ#502826](#)<sup>809</sup>
- x86: Make NMI detection work. [BZ#494120](#)<sup>810</sup>
- netback: call netdev\_features\_changed. [BZ#493092](#)<sup>811</sup>
- Invalidate dom0 pages before starting guest. [BZ#466681](#)<sup>812</sup>
- AMD IOMMU Xen pass-through support. [BZ#531469](#)<sup>813</sup>
- Add balloon driver for KVM guests. [BZ#522629](#)<sup>814</sup>
- Add AMD node ID MSR support. [BZ#530181](#)<sup>815</sup> [BZ#547518](#)<sup>816</sup>
- Provide pass-through MSI-X mask bit acceleration V3. [BZ#537734](#)<sup>817</sup>
- CD-ROM drive does not recognize new media. [BZ#221676](#)<sup>818</sup>
- kvmclock: fix incorrect wallclock value. [BZ#519771](#)<sup>819</sup>
- KMP for Xen kernel cannot be applied. [BZ#521081](#)<sup>820</sup>

A problem was found when creating KMP that includes the driver that uses the "pci\_enable\_msi/pci\_disable\_msi" function for the Xen kernel and applying it, error messages are printed out and KMP cannot be applied. This problem occurred on both i386 and x86\_64 architectures.

This update addresses this problem and these error messages no longer appear.

#### **1.88.7.1.4. Network Device Drivers**

- mlx4: pass attributes down to vlan interfaces [BZ#573098](#)<sup>821</sup>
- r8169: fix assignments in backported net\_device\_ops [BZ#568040](#)<sup>822</sup>
- virtio\_net: refill rx buffer on out-of-memory [BZ#554078](#)<sup>823</sup>
- be2net: critical bugfix from upstream [BZ#567718](#)<sup>824</sup>
- tg3: fix 5717 and 57765 asic revs panic under load [BZ#565964](#)<sup>825</sup>



- bnx2x: use single tx queue [BZ#567979](#)<sup>826</sup>
- igb: fix WoL initialization when disabled in eeprom [BZ#564102](#)<sup>827</sup>
- igb: fix warning in igb\_ethtool.c [BZ#561076](#)<sup>828</sup>
- s2io: restore ability to tx/rx vlan traffic [BZ#562732](#)<sup>829</sup>
- ixgbe: stop unmapping DMA buffers too early [BZ#568153](#)<sup>830</sup>
- e1000e: disable NFS filtering capabilities in ICH hw [BZ#558809](#)<sup>831</sup>
- bnx2: update firmware and version to 2.0.8 [BZ#561578](#)<sup>832</sup>
- mlx4: fix broken SRIOV code [BZ#567730](#)<sup>833</sup>
- mlx4: pass eth attributes down to vlan interfaces [BZ#557109](#)<sup>834</sup>
- ixgbe: initial support of ixgbe PF and VF drivers [BZ#525577](#)<sup>835</sup>
- bnx2x: update to 1.52.1-6 firmware [BZ#560556](#)<sup>836</sup>
- ixgbe: prevent speculatively processing descriptors [BZ#566309](#)<sup>837</sup>
- tg3: fix 57765 LED [BZ#566016](#)<sup>838</sup>
- tg3: fix race condition with 57765 devices [BZ#565965](#)<sup>839</sup>
- forcedeth: fix putting system into S4 [BZ#513203](#)<sup>840</sup>
- netfilter: allow changing queue length via netlink [BZ#562945](#)<sup>841</sup>
- e1000e: fix deadlock unloading module on some ICH8 [BZ#555818](#)<sup>842</sup>
- Wireless fixes from 2.6.32.2, 2.6.32.3, 2.6.32.4, & 2.6.32.7 [BZ#559711](#)<sup>843</sup>
- be2net: latest bugfixes from upstream for Red Hat Enterprise Linux 5.5 [BZ#561322](#)<sup>844</sup>
- cxgb3: add memory barriers [BZ#561957](#)<sup>845</sup>
- igb: fix msix\_other interrupt masking [BZ#552348](#)<sup>846</sup>
- niu: fix deadlock when using bondin [BZ#547943](#)<sup>847</sup>
- sky2: fix initial link state error [BZ#559329](#)<sup>848</sup>
- iptables: fix routing of REJECT target packets [BZ#548079](#)<sup>849</sup>
- niu: fix the driver to be functional with vlans [BZ#538649](#)<sup>850</sup>
- igb: update driver to support End Point DCA [BZ#513712](#)<sup>851</sup>
- tg3: update to version 3.106 for 57765 asic support [BZ#545135](#)<sup>852</sup>
- bonding: fix alb mode locking regression [BZ#533496](#)<sup>853</sup>
- e1000e: fix broken wol [BZ#557974](#)<sup>854</sup>



- fixup problems with vlans and bonding [BZ#526976](#)<sup>855</sup>
- ixgbe: upstream update to include 82599-KR support [BZ#513707](#)<sup>856</sup>
- be2net: multiple bug fixes [BZ#549460](#)<sup>857</sup>
- virtio\_net: fix tx wakeup race condition [BZ#524651](#)<sup>858</sup>
- Add support for send/receive tracepoints. [BZ#475457](#)<sup>859</sup>
- wireless: fix build when using O=objdir [BZ#546712](#)<sup>860</sup>
- update tg3 driver to version 3.100 [BZ#515312](#)<sup>861</sup>
- e1000e: support for 82567V-3 and MTU fixes [BZ#513706](#)<sup>862</sup>
- bonding: add debug module option [BZ#546624](#)<sup>863</sup>
- ipv4: fix possible invalid memory access [BZ#541213](#)<sup>864</sup>
- s2io: update driver to current upstream version [BZ#513942](#)<sup>865</sup>
- wireless: report reasonable bitrate for 802.11n [BZ#546281](#)<sup>866</sup>
- mac80211: report correct signal for non-dBm values [BZ#545899](#)<sup>867</sup>
- wireless: Remove some unnecessary warning messages. mac80211: avoid uninit pointer dereference in ieee80211. [BZ#545121](#)<sup>868</sup>
- wireless: avoid deadlock when enabling rkill [BZ#542593](#)<sup>869</sup>
- wireless: updates of mac80211 etc from 2.6.32 and wireless support updates from 2.6.32 [BZ#456943](#)<sup>870</sup>, [BZ#474328](#)<sup>871</sup>, [BZ#514661](#)<sup>872</sup> & [BZ#516859](#)<sup>873</sup>
- bnx2: update to version 2.0.2 [BZ#517377](#)<sup>874</sup>
- cnic: Update driver for Red Hat Enterprise Linux 5.5 [BZ#517378](#)<sup>875</sup>
- bnx2x: Update to 1.52.1-5, add support for bcm8727 phy, add support for bcm8727 phy, add mdio support, add firmware version 5.2.7.0 and update to 1.52.1. [BZ#515716](#)<sup>876</sup> & [BZ#522600](#)<sup>877</sup>
- mdio: Add mdio module from upstream and ethtool. Add more defines for mdio to use. Add the sfc (Solarflare) driver. [BZ#448856](#)<sup>878</sup>
- r8169: update to latest upstream for Red Hat Enterprise Linux 5.5 [BZ#540582](#)<sup>879</sup>
- benet: update driver to latest upstream for Red Hat Enterprise Linux 5.5 [BZ#515269](#)<sup>880</sup>
- e1000e: update and fix WOL issues [BZ#513706](#)<sup>881</sup>, [BZ#513930](#)<sup>882</sup>, [BZ#517593](#)<sup>883</sup> & [BZ#531086](#)<sup>884</sup>
- e1000: update to latest upstream for Red Hat Enterprise Linux 5.5 [BZ#515524](#)<sup>885</sup>
- mlx4: update to recent version with SRIOV support [BZ#503113](#)<sup>886</sup>, [BZ#512162](#)<sup>887</sup>, [BZ#520674](#)<sup>888</sup>, [BZ#527499](#)<sup>889</sup>, [BZ#529396](#)<sup>890</sup> & [BZ#534158](#)<sup>891</sup>
- ipv4: fix an unexpectedly freed skb in tcp [BZ#546402](#)<sup>892</sup>

- bnx2: fix frags index [BZ#546326](#)<sup>893</sup>
- netxen: further p3 updates for Red Hat Enterprise Linux 5.5 [BZ#542746](#)<sup>894</sup>
- netxen: driver updates from 2.6.31 and 2.6.32 [BZ#516833](#)<sup>895</sup>
- igb: update igb driver to support barton hills [BZ#513710](#)<sup>896</sup>
- enic: update to upstream version 1.1.0.100 [BZ#519086](#)<sup>897</sup>
- ipv6: synchronize closing of connections [BZ#492942](#)<sup>898</sup>
- cxgb3: fix port index issue and correct hex/decimal error [BZ#516948](#)<sup>899</sup>
- mlx4\_en: add a pci id table [BZ#508770](#)<sup>900</sup>
- resolve issues with vlan creation and filtering [BZ#521345](#)<sup>901</sup>
- gro: fix illegal merging of trailer trash [BZ#537876](#)<sup>902</sup>
- ixgbe: add and enable CONFIG\_IXGBE\_DCA [BZ#514306](#)<sup>903</sup>
- ixgbe: update to upstream version 2.0.44-k2 [BZ#513707](#)<sup>904</sup>, [BZ#514306](#)<sup>905</sup> & [BZ#516699](#)<sup>906</sup>
- call cond\_resched in rt\_run\_flush [BZ#517588](#)<sup>907</sup>
- igb: add support for 82576ns serdes adapter [BZ#517063](#)<sup>908</sup>
- qlge: updates and fixes for Red Hat Enterprise Linux 5.5 [BZ#519453](#)<sup>909</sup>
- igb: fix kexec with igb controller [BZ#527424](#)<sup>910</sup>
- qlge: fix crash with kvm guest device passthrough [BZ#507689](#)<sup>911</sup>
- igb: set vf rlpml must take vlan tag into account [BZ#515602](#)<sup>912</sup>
- fix race in data receive/select [BZ#509866](#)<sup>913</sup>
- augment raw\_send\_hdrinc to validate ihl in user hdr [BZ#500924](#)<sup>914</sup>
- bonding: introduce primary\_reselect option and ab\_arp use std active slave select code [BZ#471532](#)<sup>915</sup>
- use netlink notifications to track neighbour states and introduce generic function \_\_neigh\_notify [BZ#516589](#)<sup>916</sup>
- sched: fix panic in bnx2\_poll\_work [BZ#526481](#)<sup>917</sup>
- bnx2i/cnic: update driver version for Red Hat Enterprise Linux 5.5 [BZ#516233](#)<sup>918</sup>
- cxgb3: bug fixes from latest upstream version [BZ#510818](#)<sup>919</sup>
- sunrpc: remove flush\_workqueue from xs\_connect [BZ#495059](#)<sup>920</sup>
- lvs: adjust sync protocol handling for ipvsadm -2 and for timeout values [BZ#524129](#)<sup>921</sup>
- igb and e100: return PCI\_ERS\_RESULT\_DISCONNECT on failure [BZ#514250](#)<sup>922</sup>

- bnx2: apply BROKEN\_STATS workaround to 5706/5708 [BZ#527748](#)<sup>923</sup>
- syncookies: support for TCP options via timestamps and tcp: add IPv6 support to TCP SYN cookies [BZ#509062](#)<sup>924</sup>
- e1000e: return PCI\_ERS\_RESULT\_DISCONNECT on fail [BZ#508387](#)<sup>925</sup>
- e100: add support for 82552 [BZ#475610](#)<sup>926</sup>
- netfilter: honour source routing for LVS-NAT [BZ#491010](#)<sup>927</sup>
- Update r8169 driver to avoid losing MSI interrupts. [BZ#514589](#)<sup>928</sup>
- e1000 and ixgbe: return PCI\_ERS\_RESULT\_DISCONNECT on fail [BZ#508388](#)<sup>929</sup> & [BZ#508389](#)<sup>930</sup>
- ipt\_recent: sanity check hit count [BZ#523982](#)<sup>931</sup>
- ipv4: ip\_append\_data handle NULL routing table [BZ#520297](#)<sup>932</sup>
- fix drop monitor to not panic on null dev [BZ#523279](#)<sup>933</sup>
- ipv6: do not fwd pkts with the unspecified saddr [BZ#517899](#)<sup>934</sup>
- igbvf: recognize failure to set mac address [BZ#512469](#)<sup>935</sup>
- sunrpc client: IF for binding to a local address and set rq\_daddr in svc\_rqst on socket recv [BZ#500653](#)<sup>936</sup>
- tcp: do not use TSO/GSO when there is urgent data [BZ#502572](#)<sup>937</sup>
- vxge: new driver for Neterion 10Gb Ethernet and Makefile, Kconfig and config additions [BZ#453683](#)<sup>938</sup>
- 8139too: RTNL and flush\_scheduled\_work deadlock [BZ#487346](#)<sup>939</sup>
- icmp: fix icmp\_errors\_use\_inbound\_ifaddr sysctl [BZ#502822](#)<sup>940</sup>
- bonding: allow bond in mode balance-alb to work [BZ#487763](#)<sup>941</sup>
- rtl8139: set mac address on running device [BZ#502491](#)<sup>942</sup>
- tun: allow group ownership of TUN/TAP devices [BZ#497955](#)<sup>943</sup>
- tcp: do not use TSO/GSO when there is urgent data [BZ#497032](#)<sup>944</sup>
- A problem was found where if you set `/proc/sys/net/ipv4/route/secret_interval` to `0`, you could not reset it to another value, and `/bin/bash` would hang on the echo.  
  
The timer reschedule path was updated to ensure that the rtnl lock is always released. The `/proc/sys/net/ipv4/route/secret_interval` can now be set to `0` and successfully reset to another value without causing `/bin/bash` to hang. [BZ#510067](#)<sup>945</sup>
- sky2: revert some phy power refactoring changes [BZ#509891](#)<sup>946</sup>
- bonding: tlb/alb: set active slave when enslaving [BZ#499884](#)<sup>947</sup>
- tg3: refrain from touching MPS [BZ#516123](#)<sup>948</sup>

- qlge: fix hangs and read performance [BZ#517893](#)<sup>949</sup>
- mlx4\_en fix for vlan traffic [BZ#514141](#)<sup>950</sup>
- mlx4\_en device multi-function patch [BZ#500346](#)<sup>951</sup>
- mlx4\_core: fails to load on large systems [BZ#514147](#)<sup>952</sup>
- add DSCP netfilter target [BZ481652#](#)<sup>953</sup>

### 1.88.7.1.5. Filesystem and Storage Management Updates

#### 1.88.7.1.5.1. NFS-specific Updates

- Fix a deadlock in the sunrpc code. [BZ#548846](#)<sup>954</sup>
- Ensure `dprintk()` macro works everywhere. [BZ#532701](#)<sup>955</sup>
- Fix stale `nfs_attr` being passed to `nfs_readdir_lookup()` [BZ#531016](#)<sup>956</sup>
- Update `nfs4_do_open_expired()` to prevent infinite loops. [BZ#526888](#)<sup>957</sup>

A problem was found with `nfs4_do_open_expired()` that could lead to the reclaim thread going into an infinite loop. This bug was triggered when the client received an `NFS4ERR_DELAY` from the server, and the `exception.retry` bit was set, enforcing a timeout. This bit was never reset to zero (0) when the server recovered, leading to an infinite loop.

This update checks for server recovery and resets the `exception.retry` bit when appropriate, preventing the creation of this infinite loop.

- `nfsnobody == 4294967294` causes `idmapd` to stop responding [BZ#519184](#)<sup>958</sup>
- `statfs` on NFS partition always returns 0 [BZ#519112](#)<sup>959</sup>

A problem was found where `statfs` on NFS partitions always returned a zero (0) value, regardless of success or fail. On fail, `statfs` should return a negative number.

This update corrects the problem so that `statfs` behaves as expected.

- Read/Write NFS I/O performance was severely degraded by NFS synchronous write RPCs (`FILE_SYNC`) that occur when an application has a file open `O_RDWR` and is reading dirty pages. This `read()` system call triggered a flush of the dirty page to the server, using a 4096-byte synchronous write. The remote filesystem is mounted with an explicit `async` mount option, and the application does not open the file with `O_SYNC` or `O_DSYNC` flags.
- Mounting with a `rsz`/`wsize` of 2048 (less than the 4096 page size) eliminates these synchronous writes, and dramatically improves I/O. [BZ#498433](#)<sup>960</sup>
- `knfsd`: query fs for v4 `getattr` of `FATTR4_MAXNAME` [BZ#469689](#)<sup>961</sup>
- Bring `nfs4acl` into line with mainline code [BZ#479870](#)<sup>962</sup>
- Add an `nfsiod` workqueue [BZ#489931](#)<sup>963</sup>
- `nfsv4`: Distinguish expired from stale `stateID` [BZ#514654](#)<sup>964</sup>

- Do an exact check of attribute specified [BZ#512361](#)<sup>965</sup>

In case ACLs are not supported in the underlying filesystem, this update enables the NFSv4 server to return NFS4ERR\_ATTRNOTSUPP when ACL attributes are specified when creating a file.

- Fix regression in `nfs_open_revalidate` [BZ#511278](#)<sup>966</sup>
- Fix cache invalidation problems in `nfs_readdir` [BZ#511170](#)<sup>967</sup>

#### 1.88.7.1.5.2. GFS-specific Updates

- Fix kernel BUG when using `fiemap`. [BZ#569610](#)<sup>968</sup>
- Use correct GFP for allocating page on write. [BZ#566221](#)<sup>969</sup>

Allocation of memory during the write system call can trigger memory reclaim. This update ensures that the VM does not call back into the filesystem, resulting in a kernel OOPS. This problem is only seen in times of memory shortage on a node.

- Filesystem mounted with `ecryptfs_xattr` option could not be written. [BZ#553670](#)<sup>970</sup>
- Filesystem consistency error in `gfs2_ri_update`. [BZ#553447](#)<sup>971</sup>
- Update `O_APPEND` to behave as expected. [BZ#544342](#)<sup>972</sup>

Previously, when using GFS2, if two nodes concurrently updated the same file, each node would overwrite the other node's data, as the file position for such a file was not being updated correctly. This issue only occurred when using `open()` with the `O_APPEND` flag, and then issuing a `write()` without first performing another operation on the inode, such as `stat()` or `read()`.

- Fix glock reference count issues. [BZ#539240](#)<sup>973</sup>
- Fix rename locking issue. [BZ#538484](#)<sup>974</sup>
- Enhance `statfs` and quota usability. [BZ#529796](#)<sup>975</sup>
- Cluster failures due to invalid metadata blocks. [BZ#519049](#)<sup>976</sup>

A problem was found with `gfs2` filesystems where clusters would fail as a result of fatal filesystem withdrawal. This update provides a solution to that problem.

- `gfs2_delete_inode` failing on RO filesystem. [BZ#501359](#)<sup>977</sup>
- Fix potential race in glock code. [BZ#498976](#)<sup>978</sup>
- GFS2 ">>" will not update `ctime` and `mtime` after appending to the file. [BZ#496716](#)<sup>979</sup>
- After `gfs2_grow`, new size is not seen immediately. [BZ#482756](#)<sup>980</sup>
- Add `'-o errors=withdraw|panic'` to GFS2 mount option. [BZ#518106](#)<sup>981</sup>
- `mount.gfs` hangs forever if concurrent amount of different `gfs` filesystems are performed. [BZ#440273](#)<sup>982</sup>

#### 1.88.7.1.5.3. CIFS-specific Updates

- CIFS filesystem update, including: [BZ#562947](#)<sup>983</sup>

- Fix length calculation for converted Unicode readdir names.
- Fix dentry hash calculation for case-insensitive mounts.
- Do not make mountpoints shrinkable.
- Ensure maximum username length check in session setup matches.
- NULL out pointers when chasing DFS referrals. [BZ#544417](#)<sup>984</sup>
- Protect GlobalOplock\_Q with its own spinlock to prevent crash in small\_smb\_init. [BZ#531005](#)<sup>985</sup>
- Add new options to disable overriding of ownership. [BZ#515252](#)<sup>986</sup>
- cifs: Enable dfs submounts to handle remote referrals. [BZ#513410](#)<sup>987</sup>
- httpd Sendfile problems reading from a CIFS share. [BZ#486092](#)<sup>988</sup>
- Don't use CIFSGetSrvInodeNumber [BZ#529431](#)<sup>989</sup>
- CIFS filesystem update, including: [BZ#500838](#)<sup>990</sup>
  - Fix artificial limit on reading symlinks
  - Copy struct \*after\* setting port, not before
  - Add addr= mount option alias for ip=
  - Free nativeFileSystem before allocating new one
  - Fix read buffer overflow
  - Fix potential NULL deref in parse\_DFS\_referrals
  - Fix memory leak in ntlmv2 hash calculation
  - Fix broken mounts when an SSH tunnel is used
  - Avoid invalid kfree in cifs\_get\_tcp\_session

### 1.88.7.1.5.4. Cluster-specific Updates

- dlm: Fix connection close handling. [BZ#521093](#)<sup>991</sup>

A problem was found where a cluster would hang after a node rejoins from a simulated network outage. This update addresses the connection close handling problem that was the cause of the issue, and clusters now behave as expected in this situation.

### 1.88.7.1.5.5. Other Updates

- Fix randasys crashes x86\_64 systems regression. [BZ#562857](#)<sup>992</sup>
- proc: Make errno values consistent when race occurs. [BZ#556545](#)<sup>993</sup>
- Fix performance regression introduced by eventfd support. [BZ#548565](#)<sup>994</sup>

OLTP-type runs regressed by 0.5% due to the additional overhead in the `aio_complete()` code path.

This update uses a bit in `ki_flags` to address this problem.

- Fix possible inode corruption on unlock. [BZ#545612](#)<sup>995</sup>
- xfs: Fix fallocate error return sign. [BZ#544349](#)<sup>996</sup>

When issuing an fallocate call on xfs which results in insufficient space to complete, XFS returns "28" instead of "ENOSPC" - xfs uses positive `errno`s internally, and flips them before returning, but in this case it was missed.

This update ensures the error number is inverted before being returned.

- Skip inodes without pages to free in `drop_pagecache_sb()`. [BZ#528070](#)<sup>997</sup>
- Fix soft lockup problem with `dcache_lock`. [BZ#526612](#)<sup>998</sup>
- ext3: Replace `lock_super` with explicit resize lock. [BZ#525100](#)<sup>999</sup>

A problem was found where performing an online resize of an ext3 filesystem would fail. This update cross-ports a change developed for ext4 to address a similar problem.

- Update MPT fusion 3.4.13rh [BZ#516710](#)<sup>1000</sup>

The mtp base driver for devices using LSI Fusion MPT firmware has been updated to version 3.4.13rh. This update fixes many issues, most notably:

- The serial attached SCSI (SAS) topology scan has been restructured, adding expander, link status and host bus adapter (HBA) events.
- Intermittent issues caused by SAS cable removal and reinsertion have been fixed.
- An issue where SATA devices received different SAS addresses has been fixed.
- The device firmware now reports the queue full event to the driver and the driver handles the queue full event using the SCSI mid-layer.
- Update MPT2SAS to 02.101.00.00 [BZ#516702](#)<sup>1001</sup>

The mpt2sas driver that supports the SAS-2 family of adapters from LSI has been updated to version 02.101.00.00. This update fixes many issues, most notably:

- Sanity checks have been added when volumes are added and removed, ignoring events for foreign volumes.
- The driver is now legacy I/O port free.
- An issue that may have resulted in a kernel OOPS at hibernation or resume has been fixed.
- Fix online resize bug while using `resize2fs` [BZ#515759](#)<sup>1002</sup>
- ENOSPC during `fsstress` leads to filesystem corruption on ext2, ext3, and ext4 [BZ#515529](#)<sup>1003</sup>
- Bring `putpubfh` handling inline with upstream [BZ#515405](#)<sup>1004</sup>

- Address file write performance degradation on ext2 file systems [BZ#513136](#)<sup>1005</sup>

When file write performance is measured using the iotop benchmark test, the performance of Red Hat Enterprise Linux 5.4 GA Snapshot1 is about 40% lower than the performance of Red Hat Enterprise Linux 5.3 GA in some cases. File read performance of 5.4 GA Snapshot1 is almost the same as 5.3 GA.

This problem occurred on both i386 and x86\_64, however i386 performance degradation seemed to be worse compared to x86\_64.

This update converts ext2 to the new aops.

- getdents() reports `/proc/1/task/1/` as DT\_UNKNOWN [BZ#509713](#)<sup>1006</sup>
- Do not return invalidated nlm\_host [BZ#507549](#)<sup>1007</sup>
- Make NR\_OPEN tunable [BZ#507159](#)<sup>1008</sup>
- Free journal buffers on ext3 and ext4 file systems after releasing private data belonging to a mounted filesystem [BZ#506217](#)<sup>1009</sup>
- Prevent Genesis from getting stuck in a loop writing to an unlinked file [BZ#505331](#)<sup>1010</sup>
- Fix inode\_table test in ext{2,3}\_check\_descriptors [BZ#504797](#)<sup>1011</sup>
- Support origin size < chunk size [BZ#502965](#)<sup>1012</sup>
- smbd process hangs with flock call [BZ#502531](#)<sup>1013</sup>
- inotify: fix race [BZ#499019](#)<sup>1014</sup>
- Don't allow setting ctime over v4 [BZ#497909](#)<sup>1015</sup>
- AVC denied 0x100000 for a directory with eCryptFS and Apache [BZ#489774](#)<sup>1016</sup>
- Don't zero out pages array inside struct dio [BZ#488161](#)<sup>1017</sup>
- File truncations when both suid and write permissions are set [BZ#486975](#)<sup>1018</sup>
- Fix stripping SUID/SGID flags when chmod/chgrp directory [BZ#485099](#)<sup>1019</sup>
- Sanitize invalid partition table entries [BZ#481658](#)<sup>1020</sup>
- DIO write returns -EIO on try\_to\_release\_page fail [BZ#461100](#)<sup>1021</sup>
- Batch AIO requests [BZ#532769](#)<sup>1022</sup>
- Add eventd support. [BZ#493101](#)<sup>1023</sup>
- Update ext4 to latest upstream codebase [BZ#528054](#)<sup>1024</sup>
- If a non-root setuid binary is run as root, its `/proc/<pid>/smaps` file cannot be read because the file's permissions only allow access from a task with the original root UID value.  
  
The `/proc/<pid>/smaps` file is now created with S\_IRUGO permissions (-r--r--), which means it can be read even when running a setuid binary. [BZ#322881](#)<sup>1025</sup>



- Correctly recognize the logical unit (LU) of Hitachi-made storage. [BZ#430631](#)<sup>1026</sup>

The LU of Hitachi-made storage was not correctly recognized in Red Hat Enterprise Linux 5. The LU was correctly recognized using a combination of Red Hat Enterprise Linux 4, Hitachi-made storage, and the Qlogic-made HBA driver. Further, Red Hat Enterprise Linux 5 did recognize an LU that did not exist in the storage. The storage is used with SCSI-2.

Red Hat Enterprise Linux 5 now issues a SCSI command (REPORT\_LUN) when recognizing the logical unit in the SCSI layer. The LU is now correctly recognized when using a combination of Red Hat Enterprise Linux 5, Hitachi storage, and the Qlogic-made HBA driver.

### 1.88.7.1.6. Storage and Device Driver Updates

#### 1.88.7.1.6.1. PCI Updates

- AER: Disable advanced error reporting by default. [BZ#559978](#)<sup>1027</sup>
- Prevent PCIe AER errors being reported multiple times. [BZ#544923](#)<sup>1028</sup>

A problem was found where not all PCIe AER uncorrectable status bits were cleaned up after an uncorrectable/non-fatal or uncorrectable/fatal error was triggered. As a result, subsequent errors would sometimes display a previously reported error.

This update ensures that errors are only reported once.

- Add base AER driver support. [BZ#517093](#)<sup>1029</sup>

This feature provides the advanced error handling (diagnosis and recovery) for PCI-Express devices by adding AER (Advanced Error Reporting) support.

PCIe AER provides the finer resolution of error source and error severity, as well as the ability to reset the slot to re-initialize the device.

This update applies to 32-bit x86 and 64-bit Intel 64 and AMD64 architectures.

- Enable acs p2p upstream forwarding. [BZ#518305](#)<sup>1030</sup>

#### 1.88.7.1.6.2. SCSI Updates

- mpt2sas: Fix missing initialization. [BZ#565637](#)<sup>1031</sup>
- Update fnic and libfc to address FIP crash and hang issues. [BZ#565594](#)<sup>1032</sup>
- be2iscsi: Fix scsi eh callouts and add support for new chip to be2iscsi driver. [BZ#564145](#)<sup>1033</sup>
- device\_handler: Add netapp to ALUA device list. [BZ#562080](#)<sup>1034</sup>
- qla2xxx: Return FAILED if abort command fails. [BZ#559972](#)<sup>1035</sup>
- lpfc: Update driver to 8.2.0.63.3p FC/FCoE. [BZ#564506](#)<sup>1036</sup>
- lpfc: Update driver to 8.2.0.63.2p FC/FCoE. [BZ#557792](#)<sup>1037</sup>
- lpfc: Update driver to 8.2.0.63.1p FC/FCoE. [BZ#555604](#)<sup>1038</sup>
- be2iscsi: Upstream driver refresh for Red Hat Enterprise Linux 5.5. [BZ#554545](#)<sup>1039</sup>

- qla2xxx: Correct timeout value calculation for CT pass-through commands. [BZ#552327](#)<sup>1040</sup>
- qla2xxx driver updates. [BZ#550148](#)<sup>1041</sup>
- Update arcmsr driver to better match upstream. [BZ#521203](#)<sup>1042</sup>
- Re-enable "mpt\_msi\_enable" option. [BZ#520820](#)<sup>1043</sup>
- Kernel panics from list corruption when using a tape drive connected through cciss adapter. [BZ#520192](#)<sup>1044</sup>
- lpfc: Update version from 8.2.0.52 to 8.2.0.59. [BZ#516541](#)<sup>1045</sup> [BZ#529244](#)<sup>1046</sup>
- megaraid: Make driver legacy I/O port free. [BZ#515863](#)<sup>1047</sup>
- Update Emulex lpfc 8.2.0.x FC/FCoE driver. [BZ#515272](#)<sup>1048</sup>
- scsi\_transport\_fc: fc\_user\_scan correction to prevent scsi\_scan looping forever. [BZ#515176](#)<sup>1049</sup>
- Update qla2xxx qla4xx driver. [BZ#519447](#)<sup>1050</sup>
- Update for HighPoint RocketRAID hptiop driver. [BZ#519076](#)<sup>1051</sup>
- Errata 28 fix on LSI53C1030. [BZ#](#)<sup>1052</sup>
- Add kernel (scsi\_dh\_rdace) support for Sun 6540 storage arrays. [BZ#518496](#)<sup>1053</sup>
- Disable state transition from OFFLINE to RUNNING. [BZ#516934](#)<sup>1054</sup>

This feature prevents a timeout from occurring on the same device repeatedly by disabling the state transition of the SCSI device from OFFLINE to RUNNING in the `unblock` function of the SCSI layer.

This update applies to 32-bit x86, 64-bit Intel 64 and AMD64, and 64-bit Itanium2 architectures.

- Add be2iscsi driver. [BZ#515284](#)<sup>1055</sup>
- Add emc clarion support to scsi\_dh modules. [BZ#437107](#)<sup>1056</sup>
- scsi\_dh\_rdac driver update. [BZ#524335](#)<sup>1057</sup>
- qla2xxx: Allow use of MSI when MSI-X disabled. [BZ#517922](#)<sup>1058</sup>

On Red Hat Enterprise Linux 5 the MSI-X disable option for this driver also disables MSI. This update adds another state to the variable to allow the user to specify either MSI or MSI-X.

### 1.88.7.1.6.3. Other Updates

- Add Support for Huawei EC1260. [BZ#517454](#)<sup>1059</sup>
- Update stex driver to version 4.6.0102.4. [BZ#516881](#)<sup>1060</sup>
- Add support for the hp-ilo driver. [BZ#515010](#)<sup>1061</sup>
- Include support for SB900 SATA/IDE controllers. [BZ#515114](#)<sup>1062</sup>
- qla2xxx: add AER support. [BZ#513927](#)<sup>1063</sup>

- Add bfa Brocade BFA Fibre-Channel/FCoE driver. [BZ#475695](#)<sup>1064</sup>
- Add pmcraid driver. [BZ#529979](#)<sup>1065</sup>
- Update lpfc driver. [BZ#549763](#)<sup>1066</sup>
- Update megaraid driver. [BZ#518243](#)<sup>1067</sup>

#### 1.88.7.1.7. Block Device Updates

- cfq-iosched: Fix sequential read performance regression. [BZ#571818](#)<sup>1068</sup>
- cfq: Kick busy queues without waiting for merged req. [BZ#570814](#)<sup>1069</sup>
- raid45: Fix for kernel OOPS resulting from constructor error path. [BZ#565494](#)<sup>1070</sup>
- Fix deadlock at suspending mirror device. [BZ#555120](#)<sup>1071</sup>
- Fix I/O errors while accessing loop devices or file-based Xen images from GFS volume. [BZ#549397](#)<sup>1072</sup>
- Correct issue with MD/DM mapping in blktrace. [BZ#515551](#)<sup>1073</sup>
- Fix install panic with xen iSCSI boot device. [BZ#512991](#)<sup>1074</sup>
- Allow more flexibility for read\_ahead\_kb store. [BZ#510257](#)<sup>1075</sup>
- Add device ID for 82801JI sata controller. [BZ#506200](#)<sup>1076</sup>
- Fix a race in dm-raid1. [BZ#502927](#)<sup>1077</sup>
- raid: deal with soft lockups during resync. [BZ#501075](#)<sup>1078</sup>
- blktrace stops working after a trace-file-directory replacement. [BZ#498489](#)<sup>1079</sup>
- I/O scheduler setting via elevator kernel option is not picked up by Xen guest. [BZ#498461](#)<sup>1080</sup>
- Fix rcu accesses in partition statistics code. [BZ#493517](#)<sup>1081</sup>
- Fix iosched batching fairness and reset batch for ordered requests. [BZ#462472](#)<sup>1082</sup>

#### 1.88.7.1.8. Multiple Device Updates

- Fix kernel panic releasing bio structure after recovery failed. [BZ#555171](#)<sup>1083</sup>
- Lock snapshot while reporting status. [BZ#543307](#)<sup>1084</sup>

A problem was found where, in the `snapshot_status()` function, the counts were being read without holding the lock. This could result in invalid intermediate values being reported.

This update is a backport of a previous patch that locks the snapshot while reporting status.

- Fix deadlock in device mapper multipath when removing a device. [BZ#543270](#)<sup>1085</sup>
- Snapshots of the same origin with differing chunk sizes causes corruption. [BZ#210490](#)<sup>1086</sup>

The kernel driver dm-snapshot handles multiple snapshots with different chunk sizes incorrectly. It occasionally dispatches write requests to the origin volume prior to copying the data to all the snapshots. As a consequence, the snapshots are not static and writes to the origin are occasionally reflected to the snapshots. When there are multiple snapshots of the same origin volume with different chunk sizes, and you write to the origin volume, the data in the snapshots may be corrupted.

This update ensures that the kernel driver always waits until all the chunks in all the snapshots are reallocated before dispatching a write request to the origin device.

- raid5: Mark cancelled readahead BIOS with -EIO. [BZ#512552](#)<sup>1087</sup>

### 1.88.7.1.9. Wireless Infrastructure and Driver Updates

- iwlmwifi: Fix dual-band N-only use on IWL5x00. [BZ#566696](#)<sup>1088</sup>
- rt2x00: Fix work cancel race conditions. [BZ#562972](#)<sup>1089</sup>
- Update old static regulatory domain rules. [BZ#543723](#)<sup>1090</sup>
- Puma Peak wireless support. [BZ#516859](#)<sup>1091</sup>

This update contains support for the iwl6000 hardware from Intel. Devices in this hardware line support 802.11a, 802.11b, 802.11g, and 802.11n protocols. This update also includes support for the iwl1000 hardware line. Support for iwl5000, iwl4965, and iwl3945 was also updated.

In order to support the features of these drivers, the mac80211 and cfg80211 subsystems were updated. Further, all existing mac80211-based drivers were refreshed to match the updated mac80211 subsystem.

- Support Realtek RTL8187B wireless driver. [BZ#514661](#)<sup>1092</sup>
- Update Intel wireless driver (iwlagn) for iwl4965 / iwl5000. [BZ#474328](#)<sup>1093</sup>
- Add support for Atheros wireless ATH9k driver. [BZ#456943](#)<sup>1094</sup>

The update of the mac80211 enabled support of the ath9k driver. This supports the full line of 802.11n wireless LAN adapters from Atheros.

- mac80211: fix reported wireless extensions version. [BZ#513430](#)<sup>1095</sup>

### 1.88.7.1.10. Memory Management Updates

- [Xen] mmap( ) with PROT\_WRITE on Red Hat Enterprise Linux 5 was incompatible with Red Hat Enterprise Linux 4. [BZ#562761](#)<sup>1096</sup>
- munmap( ) fails when mm\_struct.map\_count temporarily reaches max\_map\_count [BZ#552648](#)<sup>1097</sup>

A problem was found where munmap( ) would fail with an ENOMEM error if:

- the number of VMAs = VMA limit - 1, and
- it does not unmap an entire VMA but only part of a VMA.

This update implements further checks to handle partial unmappings to avoid this problem.

- Update `ioremap` to prevent kernel hang when using recent NVIDIA display drivers. [BZ#549465](#)<sup>1098</sup>

A problem was found where attempting to run a recent NVIDIA display driver on 32-bit Red Hat Enterprise Linux 5.3 or 5.4 would cause the kernel to hang. This was due to hitting a `BUG()` call in the `__change_page_attr()` routine.

This update provides the necessary changes to address this problem.

- Prevent hangs during memory reclaim on large systems. [BZ#546428](#)<sup>1099</sup>
- Call `vfs_check_frozen()` after unlocking the spinlock. [BZ#541956](#)<sup>1100</sup>
- Display UID as well as PID in OOM killer output. [BZ#520419](#)<sup>1101</sup>
- AMD-IOMMU: Support more IOMMU parameters and rework interrupt remapping according to IOMMU spec 1.26. [BZ#518474](#)<sup>1102</sup> [BZ#526766](#)<sup>1103</sup>
- Add a tracepoint for kernel pagefault events. [BZ#517133](#)<sup>1104</sup>

This feature provides a tracepoint to trace kernel pagefault events. The argument should include the IP (instruction pointer) and the faulted virtual address.

This update applies to 32-bit x86 and 64-bit Intel 64 and AMD64 architectures.

- Memory mapped files not updating timestamps. [BZ#452129](#)<sup>1105</sup>
- Prevent hangs or long pauses when `zone_reclaim_mode=1`. [BZ#507360](#)<sup>1106</sup>

### 1.88.7.1.11. Audit and Security Updates

#### 1.88.7.1.11.1. Audit Updates

- Fix breakage and leaks in `audit_tree.c` [BZ#549750](#)<sup>1107</sup>

A problem was found where if a user ran `auditctl -R audit.rules` which unloads and then loads rules that include (for example) `"-F dir=/var/log/audit"` or `"-F dir=/lib"`, it would result in a kernel OOPS.

This update provides a fix for this issue.

- Correct the record length of `execve`. [BZ#509134](#)<sup>1108</sup>

#### 1.88.7.1.11.2. Cryptography Updates

- IBM S/390: Permit weak keys unless `REQ_WEAK_KEY` is set. [BZ#504667](#)<sup>1109</sup>

#### 1.88.7.1.11.3. SELinux Updates

- Update `audit_update_watch()` to prevent system crashes while running `usermod`. [BZ#526819](#)<sup>1110</sup>
- Allow preemption between transition permission checks in order to prevent CPU soft lockup [BZ#516216](#)<sup>1111</sup>

A problem was found where the kernel would sometimes go into a soft lockup for 10s at `.context_struct_compute_av+0x214/0x39c`. This update changes the way transition checks are performed in order to avoid this problem.

### 1.88.7.1.12. Miscellaneous Updates

- `power_meter`: Avoid OOPS on driver load. [BZ#566575](#)<sup>1112</sup>
- `hvc_iucv`: Allocate IUCV send/receive buffers in DMA zone. [BZ#566202](#)<sup>1113</sup>
- `f71805f`: Fix `sio_data` to `platform_device_add_data()`. [BZ#564399](#)<sup>1114</sup>
- Fix 32-bit Machine Check Exception Handler. [BZ#562862](#)<sup>1115</sup>
- Fix APIC and TSC reads for guests. [BZ#562006](#)<sup>1116</sup>
- `zcrypt`: Do not remove coprocessor in case of error 8/72. [BZ#561067](#)<sup>1117</sup>
- `smc47m1`: Fix data to `platform_device_add_data()`. [BZ#560944](#)<sup>1118</sup>
- `it87`: Fix `sio_data` to `platform_device_add_data()`. [BZ#559950](#)<sup>1119</sup>
- `w83627hf`: Fix data to `platform_device_add_data()`. [BZ#557172](#)<sup>1120</sup>
- Power Now driver: fix crash on AMD family 0x11 processors. [BZ#555180](#)<sup>1121</sup>
- EDAC driver fix for non-MMCONFIG systems. [BZ#550123](#)<sup>1122</sup>
- `khungtaskd` not stopped during suspend. [BZ#550014](#)<sup>1123</sup>
- Do not evaluate `WARN_ON` condition twice. [BZ#548653](#)<sup>1124</sup>
- Fix NULL pointer panic in `acpi_run_os`. [BZ#547733](#)<sup>1125</sup>
- Implement public `pci_ioremap_bar` function. [BZ#546244](#)<sup>1126</sup>
- Fix `PTTRACE_KILL` hanging in 100% CPU loop. [BZ#544138](#)<sup>1127</sup>
- Fix compile warnings in `eeh` code. [BZ#538407](#)<sup>1128</sup>

This update was necessary to address a compile problem in PowerPC introduced by a change in the PCI AER code.

- [infiniband] Fix bitmask handling from QP control block. [BZ#561953](#)<sup>1129</sup>
- [infiniband] Fix issue with sleep in interrupt ehca handler. [BZ#561952](#)<sup>1130</sup>
- [infiniband] Rewrite SG handling for RDMA logic. [BZ#540686](#)<sup>1131</sup>

After dma-mapping an SG list provided by the SCSI midlayer, user must ensure the mapped SG is "aligned for RDMA", in the sense that it is possible to produce one mapping in the HCA IOMMU which represents the whole SG. Next, the mapped SG is formatted for registration with the HCA.

This update provides the necessary rewrites to achieve the above.

- [infiniband] `init neigh->dgid.raw` on bonding events. [BZ#538067](#)<sup>1132</sup>

This update was necessary to address an issue found where, using IPoIB, connectivity would be lost with a single host but maintained with other hosts.

- USB driver update. [BZ#537433](#)<sup>1133</sup>

This driver update avoids USB 1.1 device failures that may occur due to requests from USB OHCI controllers being overwritten if the latency for any pending request by the USB controller is very long (in the range of milliseconds).

- Add qcserial module to Red Hat Enterprise Linux 5 kernel. [BZ#523888](#)<sup>1134</sup>

This module was added to support the Qualcomm WWAN cards used by some laptops.

- sysctl: Require CAP\_SYS\_RAWIO to set mmap\_min\_addr. [BZ#534018](#)<sup>1135</sup>

- Enable msi-x correctly on qllogic 2xxx series. [BZ#531593](#)<sup>1136</sup>

This update enables the FC and FCoE drivers to use MSI-X or MSI interrupts when they are available. The ql2xenablesix can be used to override this:

```
0 = enable traditional pin-based interrupt mechanism
1 = enable MSI-X interrupt mechanism
2 = enable MSI interrupt mechanism
```

- Implement futex priority-based wakeup. [BZ#531552](#)<sup>1137</sup>

A problem was found where the threads waiting on the futex\_q queue list would acquire the mutex lock in the order they were queued rather than by priority. This update addresses that problem.

- Make scsi\_dh\_activate() asynchronous to address the slower LUN failovers with large numbers of LUNs. [BZ#537514](#)<sup>1138</sup>

- [scsi] Fix inconsistent usage of max\_lun [BZ#531488](#)<sup>1139</sup>

- Fix dlm\_recv deadlock under memory pressure while processing GFP\_KERNEL locks. [BZ#530537](#)<sup>1140</sup>

- [scsi] Panic at .ipr\_sata\_reset after device reset. [BZ#528175](#)<sup>1141</sup>

- [scsi] Export scsilun\_to\_int symbol. [BZ#528153](#)<sup>1142</sup>

This symbol is needed by some drivers, and without this update they each tend to use their own copy of the entire function.

- Ensure pci\_dev->is\_enabled is set. [BZ#527496](#)<sup>1143</sup>

Failure to set this may cause suspend/resume to fail on some devices.

- Fix a bug in rwsem\_is\_locked() function. [BZ#526092](#)<sup>1144</sup>

- [scsi] cciss: Ignore stale commands after reboot. [BZ#525440](#)<sup>1145</sup>

- Fix a mistake in ACPI debug statement that prevents kernel compilation. [BZ#524787](#)<sup>1146</sup>

- Fix panic in cpufreq\_get on DL785-G6. [BZ#523505](#)<sup>1147</sup>

A problem was found in `cpufreq_get` which sometimes causes a kernel panic on HP DL785-G6 machines running Red Hat Enterprise Linux 5.3 and 5.4.

This update addresses the problem that was occurring and this kernel panic no longer occurs.

- [FIPS140-2] Provide option to disable/enable use of the first random block. [BZ#523259](#)<sup>1148</sup>
- [FIPS140-2] Do not use the first n-bit block generated after power-up, initialization, or reset. [BZ#522860](#)<sup>1149</sup>
- `thinkpad_acpi`: Disable `ecnvram` brightness. [BZ#522745](#)<sup>1150</sup>

The brightness of the screen needed to be manually set using the "Fn + Home" key combination every time you reboot an IBM T43 laptop, using the Intel Corporation Mobile 915GM/GMS/910GML Express Graphics Controller (rev 03). This problem was traced to the fact that the `thinkpad_acpi` CMOS NVRAM (7) and EC (5) did not agree on the display brightness level.

This update addresses this problem and the screen now always starts at the highest brightness setting.

- `pciehp`: Fix PCI-E hotplug slot detection. [BZ#521731](#)<sup>1151</sup>

A problem was found where the PCI-E hotplug slot was not detected by the `pciehp` driver on some platforms. The cause of this problem was traced to a bug in the `pciehp` driver. This update addresses this bug and PCI-E hotplug slots are now detected correctly.

- Fix NULL pointer dereference in `pci_bus_show_cpuaffinity()` [BZ#519633](#)<sup>1152</sup>

A problem was found where reading `/sys/class/pci_bus/0000:ff/cpuaffinity` (using `cat` or a similar function) would cause the kernel to crash and the system to reboot. This update provides a solution to this problem.

- Fix device detach and hotplug with `iommu=pt` [BZ#516811](#)<sup>1153</sup> [BZ#518103](#)<sup>1154</sup>

A problem was found with `iommu=pt` mode for `intel_iommu` where if you are using `iommu=pt` and you assign a device to a KVM guest and then de-assign it, the result is a device which is not usable in the host. It can be re-assigned to other guests again, but not directly used in the host.

There is also an issue where with `iommu=pt` any PCI devices that are hot-plugged in the host cannot be used.

This update provides a solution to the above problems.

- [firewire] `fw-ohci`: Fix IOMMU resource exhaustion. [BZ#513827](#)<sup>1155</sup>
- Support AMD Magny-Cours power-aware scheduler fix. [BZ#513685](#)<sup>1156</sup>
- Fix CPU `llc_shared_map` information. [BZ#513684](#)<sup>1157</sup>
- [cpufreq] Add option to avoid smi while calibrating. [BZ#513649](#)<sup>1158</sup>

The CPU frequency (`cpu_khz`) was infrequently calculated as larger value than the CPU's specification in both Red Hat Enterprise Linux 5.1(x86) and 5.2(x86). This also contributed to the system time being gradually delayed. This update adds an option to avoid this problem.



- [cpufreq] Don't set policy for offline CPUs. [BZ#511211](#)<sup>1159</sup>
- Add CPU hotplug notifiers to support suspend-to-disk and suspend-to-RAM while using KVM. [BZ#510814](#)<sup>1160</sup>
- Better FASYNC handling on file close. [BZ#510746](#)<sup>1161</sup>
- fd leak if pipe() is called with an invalid address. [BZ#509625](#)<sup>1162</sup>
- Kernel panic occurs when adding nosmp option and booting the system. [BZ#509581](#)<sup>1163</sup>
- Increase hibernate timeout. [BZ#507331](#)<sup>1164</sup>
- Hang on boot due to wrong APIC timer calibration. [BZ#503957](#)<sup>1165</sup>
- DASD failfast flag cannot be set on. [BZ#503222](#)<sup>1166</sup>
- wacom: add Intuos4 support. [BZ#502708](#)<sup>1167</sup>
- st: display current settings of option bits. [BZ#501030](#)<sup>1168</sup>
- psmouse: reenable mouse on shutdown. [BZ#501025](#)<sup>1169</sup>
- Relocate initramfs to increase vmalloc space. [BZ#499253](#)<sup>1170</sup>
- Fix undefined reference to `\_\_udivdi3'. [BZ#499063](#)<sup>1171</sup>
- Add Oprofile support for Nehalem-EP processors. [BZ#498624](#)<sup>1172</sup>
- Multiple device failure renders dm-raid1 unfixable. [BZ#498532](#)<sup>1173</sup>
- Don't oomkill when hugepage alloc fails on node. [BZ#498510](#)<sup>1174</sup>
- Prevent tmpfs from going readonly during oom kills. [BZ#497257](#)<sup>1175</sup>
- documentation: fix file-nr definition in fs.txt. [BZ#497200](#)<sup>1176</sup>
- Conditional flush in flush\_all\_zero\_pkmmaps. [BZ#484683](#)<sup>1177</sup>
- Fix corrupted intel\_rng kernel messages. [BZ#477778](#)<sup>1178</sup>
- Use KVM pvclock code to detect/correct lost ticks. [BZ#476075](#)<sup>1179</sup>
- Fix mcp55 apic routing. [BZ#473404](#)<sup>1180</sup>
- Fix snapshot crash on invalidation. [BZ#461506](#)<sup>1181</sup>
- Add pci\_domain\_nr. [BZ#450121](#)<sup>1182</sup>
- hwmon: Update to latest upstream for Red Hat Enterprise Linux 5.5. [BZ#467994](#)<sup>1183</sup> [BZ#250561](#)<sup>1184</sup> [BZ#446061](#)<sup>1185</sup>
- LRO (Large Receive Offload) is a network technology that offloads some of the overhead associated with receiving high-volume traffic from a single host. Though there is a performance benefit to LRO it cannot be used in environments where the host will take the incoming traffic and forward it to another device on the system (internal or external). In such environments, the host will panic when LRO is enabled on an interface and that interface is placed into a bridge on the host.

A check was placed in an additional portion of the bridge forwarding code and the following message (or similar) will be printed to the console or logs when a device with LRO enabled is placed into a bridge on the host or has routing enabled: "eth0: received packets cannot be forwarded while LRO is enabled". [BZ#483646](#)<sup>1186</sup>

- jbd slab cache creation/deletion is racey. [BZ#496847](#)<sup>1187</sup>
- In some cases, kernel panics while calling SysRQ-C. The printk warning about long delays was removed, and the kernel no longer hangs when SysRQ-C is called. [BZ#497195](#)<sup>1188</sup>
- Fix serial ports on IBM Point-of-Sale hardware. [BZ#506799](#)<sup>1189</sup>
- Add support for Intel multi-APIC-cluster systems. [BZ#507333](#)<sup>1190</sup>
- A bug was found in `ia64_mca_modify_original_stack` (`arch/ia64/kernel/mca.c`) where if INIT was issued while the kernel was in `fsys-mode`, the register was not saved in the stack. Consequently, the `kdump` corefile could not be backtraced in IA64. Registers in the stack are now restored on init. [BZ#515753](#)<sup>1191</sup>
- Add a tracepoint for the `coredump` event to the kernel. The new tracepoint provides tracing tools with pointers to the `coredump` filename string, and to the `coredump_params` data structure. [BZ#517115](#)<sup>1192</sup>
- Add four new signal-related tracepoints to the kernel. These tracepoints provide tracing tools which can deliver significant amounts of data. Refer to the bug report for full details. [BZ#517121](#)<sup>1193</sup>
- Add support for Nehalem-EX (Beckton) processors in Oprofile. [BZ#521992](#)<sup>1194</sup>

## 1.89. kexec-tools

### 1.89.1. RHBA-2009:1600: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1600](#)<sup>1195</sup>

An updated `kexec-tools` package that fixes various bugs is now available.

`kexec-tools` provides the `/sbin/kexec` binary that facilitates a new kernel to boot using the kernel's `kexec` feature either on a normal or a panic reboot. This package contains the `/sbin/kexec` binary and ancillary utilities that together form the user-space component of the kernel's `kexec` feature.

This updated `kexec-tools` package includes fixes for the following bugs:

\* when the bonding network driver was configured on a system running as `dom0` with the `kernel-xen` kernel, sending a `vmcore` file via the bonded interface failed due to a `mkdumprd` misconfiguration, resulting in a loss of the core. With this update, sending a `vmcore` file on a `dom0` system with `kdump`

configured to send it via the bonded interface works as expected, and the resulting core is transferred successfully. ([BZ#532030](#)<sup>1196</sup>)

\* kdump could create a truncated or zero-length vmcore file on large-memory systems. This was due to the amount of system RAM causing the creation of more than thirty-two E820 map entries in the BIOS, which in turn led kexec to truncate that list, thus causing memory to be ignored during kdump boot, and eventually resulting in truncated or zero-length vmcore files. With this update, kdump is now aware of this potential situation on large-memory systems, with the result that vmcore files are created correctly, without being truncated or zero in length. ([BZ#533793](#)<sup>1197</sup>)

All users of kexec-tools are advised to upgrade to this updated package, which resolves these issues.

## 1.89.2. RHBA-2010:0179: bug fix update

An updated kexec-tools package that fixes numerous bugs is now available.

kexec-tools provides kexec binary that facilitates a new kernel to boot using the kernel's kexec feature either on a normal or a panic reboot, together with ancillary utilities that form the userspace component of the kernel's kexec feature

This update addresses the following issues:

\* previously, the kdump kernel command line supported a "mem=" parameter that limited the memory that was dumped. When this parameter was set, the dump would result in an I/O error. The "mem=" parameter has been removed from kexec to ensure that core dumps succeed. ([BZ#239791](#)<sup>1198</sup>)

\* previously kdump waited indefinitely for all devices in its critical\_disks list to be available before it performed a dump. Kexec-tools now has a disk\_timeout parameter that limits how long kdump will wait for storage to respond. ([BZ#500741](#)<sup>1199</sup>)

\* a logical flaw meant that the presence of files with certain names in current directory of mkdumprd would prevent a dump. The code used to evaluate the remote server name has been corrected. ([BZ#509404](#)<sup>1200</sup>)

\* host names specified in the kdump.conf script needs to be entered as fully-qualified domain names to allow for DNS changes. The documentation for kdump has been revised to make this requirement clear. ([BZ#510816](#)<sup>1201</sup>)

\* previously, the vmcore file created by starting kdump with an initscript used the "--sparse=always" option when copying, resulting in a smaller file. The same option has now been added as a default value in the kdump.conf configuration file, ensuring that the default behavior is consistent. ([BZ#511003](#)<sup>1202</sup>)

\* previously, faulty logic in the code that cleans up files used by kdump in /tmp meant that files were sometimes left behind in /tmp. This has been corrected to ensure that files in /tmp are cleaned up. ([BZ#512098](#)<sup>1203</sup>)

---

<sup>1196</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=532030](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=532030)

<sup>1197</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=533793](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=533793)

<sup>1198</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=239791](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=239791)

<sup>1199</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=500741](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=500741)

<sup>1200</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=509404](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=509404)

<sup>1201</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=510816](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=510816)

<sup>1202</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=511003](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=511003)

<sup>1203</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=512098](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=512098)

- \* previously, the order in which kdump loaded storage drivers meant that USB-attached storage was sometimes not correctly detected. The USB driver is now loaded later in the boot sequence, so that device enumeration is correct and that dumps takes place successfully. ([BZ#513608](https://bugzilla.redhat.com/show_bug.cgi?id=513608)<sup>1204</sup>)
- \* Makedumpfiles can now accept kdump compressed dumps, therefore allowing users to transfer smaller files. ([BZ#516877](https://bugzilla.redhat.com/show_bug.cgi?id=516877)<sup>1205</sup>)
- \* previously, the code used by kdump to find network interfaces could not correctly identify slaves in a Xen environment when the dom0 was configured for bonding. The code has now been updated so that it recognizes this type of interface. ([BZ#516907](https://bugzilla.redhat.com/show_bug.cgi?id=516907)<sup>1206</sup>)
- \* Previously, the sample grub.conf file provided in the kexec-kdump-howto.txt omitted the "crashkernel" parameter. The sample file now describes a correctly configured grub.conf. ([BZ#531244](https://bugzilla.redhat.com/show_bug.cgi?id=531244)<sup>1207</sup>)
- \* Kexec now supports Enhanced Disk Drive Services (EDD) and up to 128 memory ranges from BIOS, so dumps on recent Intel 64-bit platforms now complete successfully. ([BZ#531340](https://bugzilla.redhat.com/show_bug.cgi?id=531340)<sup>1208</sup>)
- \* previously, kdump did not test to see whether an NFS location was writeable before commencing a dump. If the location was unwritable, kdump would therefore start the dump anyway, which would inevitably fail. Kdump now checks that NFS locations are writeable. ([BZ#533565](https://bugzilla.redhat.com/show_bug.cgi?id=533565)<sup>1209</sup>)
- \* previously, mkdumprd resolved hostnames for NFS locations specified in kdump.conf and stored their IP addresses. Mkdumprd now stores the hostnames instead and can therefore find the hosts successfully even if their IP addresses change. ([BZ#545980](https://bugzilla.redhat.com/show_bug.cgi?id=545980)<sup>1210</sup>)
- \* kexec-tools now pulls in nsslibs and using the settings in /etc/resolv.conf, can therefore perform DNS lookups and find NFS locations specified in kdump.conf. ([BZ#549946](https://bugzilla.redhat.com/show_bug.cgi?id=549946)<sup>1211</sup>)
- \* a reference to libc.so.6 has now been removed for Itanium systems. This avoids a potentially confusing warning message. ([BZ#559126](https://bugzilla.redhat.com/show_bug.cgi?id=559126)<sup>1212</sup>)
- \* a recent reorganization of the library directories on PowerPC systems placed glibc in /lib/power6x, although libnss files expected it to be in /lib. The correct path is now explicitly provided in mkdumprd, so DNS lookups work on PowerPC systems. ([BZ#569119](https://bugzilla.redhat.com/show_bug.cgi?id=569119)<sup>1213</sup>)

All kexec-tools users should upgrade to this updated package, which resolves these issues.

---

<sup>1204</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=513608](https://bugzilla.redhat.com/show_bug.cgi?id=513608)

<sup>1205</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=516877](https://bugzilla.redhat.com/show_bug.cgi?id=516877)

<sup>1206</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=516907](https://bugzilla.redhat.com/show_bug.cgi?id=516907)

<sup>1207</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=531244](https://bugzilla.redhat.com/show_bug.cgi?id=531244)

<sup>1208</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=531340](https://bugzilla.redhat.com/show_bug.cgi?id=531340)

<sup>1209</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=533565](https://bugzilla.redhat.com/show_bug.cgi?id=533565)

<sup>1210</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=545980](https://bugzilla.redhat.com/show_bug.cgi?id=545980)

<sup>1211</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=549946](https://bugzilla.redhat.com/show_bug.cgi?id=549946)

<sup>1212</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=559126](https://bugzilla.redhat.com/show_bug.cgi?id=559126)

<sup>1213</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=569119](https://bugzilla.redhat.com/show_bug.cgi?id=569119)

## 1.90. krb5

### 1.90.1. RHSA-2010:0029: Critical security update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2010:0029](#)<sup>1214</sup>

Updated krb5 packages that fix multiple security issues are now available for Red Hat Enterprise Linux 3, 4, and 5, and Red Hat Enterprise Linux 4.7, 5.2, and 5.3 Extended Update Support.

This update has been rated as having critical security impact by the Red Hat Security Response Team.

Kerberos is a network authentication system which allows clients and servers to authenticate to each other using symmetric encryption and a trusted third party, the Key Distribution Center (KDC).

Multiple integer underflow flaws, leading to heap-based corruption, were found in the way the MIT Kerberos Key Distribution Center (KDC) decrypted ciphertexts encrypted with the Advanced Encryption Standard (AES) and ARCFOUR (RC4) encryption algorithms. If a remote KDC client were able to provide a specially-crafted AES- or RC4-encrypted ciphertext or texts, it could potentially lead to either a denial of service of the central KDC (KDC crash or abort upon processing the crafted ciphertext), or arbitrary code execution with the privileges of the KDC (i.e., root privileges). ([CVE-2009-4212](#)<sup>1215</sup>)

All krb5 users should upgrade to these updated packages, which contain a backported patch to correct these issues. All running services using the MIT Kerberos libraries must be restarted for the update to take effect.

## 1.91. ksh

### 1.91.1. RHBA-2009:1686: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1686](#)<sup>1216</sup>

An updated ksh package that fixes two bugs is now available.

KSH-93 is the most recent version of the KornShell by David Korn of AT&T Bell Laboratories. KornShell is a shell programming language which is also compatible with "sh", the original Bourne Shell.

This updated ksh package includes fixes for the following bugs:

<sup>1215</sup> <https://www.redhat.com/security/data/cve/CVE-2009-4212.html>

\* when a ksh script included multibyte characters, ksh's script parser then failed to parse the script and printed a "syntax error" message. This updated package corrects this error: ksh's script parser now correctly handles multibyte characters and no error is returned when they are found. ([BZ#543447](https://bugzilla.redhat.com/show_bug.cgi?id=543447)<sup>1217</sup>)

\* the ksh shell uses a special variable, "\$!", which contains the process ID (pid) of the last background job or background function. However, the \$! variable did not contain the correct pid when it was called within a ksh function (defined with the "function" syntax). With this update, referencing the \$! special variable works as expected and the correct process ID of the last background job or function is returned, even when it is referenced from within a ksh script function. ([BZ#544974](https://bugzilla.redhat.com/show_bug.cgi?id=544974)<sup>1218</sup>)

All KornShell users are advised to upgrade to this updated package, which resolves these issues.

### 1.91.2. RHBA-2010:0234: bug fix and enhancement update

An updated Ksh package that fixes various bugs is now available.

KSH-93 is the most recent version of the KornShell by David Korn of AT&T Bell Laboratories -- a shell programming language upwards-compatible with "sh" (the Bourne Shell).

This updated ksh package upgrades ksh to the more recent 2010-02-02 upstream version (release ksh93t+) In addition, this updated ksh package addresses the following bugs:

\* running ksh scripts for a long time on an overloaded system resulted in a race condition caused by an inner linear job list getting looped. This resulted in ksh utilizing 100 % of the cpu capacity. Some operations on the job list were reordered to prevent this race condition occurring, allowing ksh scripts to be run normally on the system. ([BZ#435159](https://bugzilla.redhat.com/show_bug.cgi?id=435159)<sup>1219</sup>)

\* when .profile executed a return command, some new processes were executed without working stdin, because it was already closed. This version correctly restores the shell state after return was used in .profile making stdin available for new processes. ([BZ#506790](https://bugzilla.redhat.com/show_bug.cgi?id=506790)<sup>1220</sup>)

\* ksh returned an incorrect exit code of one when unsetting a variable that was already unset. Ksh now returns zero exit code. ([BZ#508869](https://bugzilla.redhat.com/show_bug.cgi?id=508869)<sup>1221</sup>)

\* when a parent of a background process was completed, ksh did not wait for output of the background process. Ksh now waits for the output of the background process so preventing the loss of data. ([BZ#509326](https://bugzilla.redhat.com/show_bug.cgi?id=509326)<sup>1222</sup>)

\* when emacs editing mode was used and an alias was set, it was sometimes evaluated too early causing a syntax error. Aliases are evaluated later in the process now which prevents false positive syntax errors. ([BZ#513967](https://bugzilla.redhat.com/show_bug.cgi?id=513967)<sup>1223</sup>)

\* ksh indicated commands in the man page that are not available. Man page is now amended to indicate that these commands are not available on Linux systems. ([BZ#514485](https://bugzilla.redhat.com/show_bug.cgi?id=514485)<sup>1224</sup>)

\* the ksh shell uses a special variable, "\$!", which contains the process ID (pid) of the last background job or background function. However, the \$! variable did not contain the correct pid when it was

---

<sup>1217</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=543447](https://bugzilla.redhat.com/show_bug.cgi?id=543447)

<sup>1218</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=544974](https://bugzilla.redhat.com/show_bug.cgi?id=544974)

<sup>1219</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=435159](https://bugzilla.redhat.com/show_bug.cgi?id=435159)

<sup>1220</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=506790](https://bugzilla.redhat.com/show_bug.cgi?id=506790)

<sup>1221</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=508869](https://bugzilla.redhat.com/show_bug.cgi?id=508869)

<sup>1222</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=509326](https://bugzilla.redhat.com/show_bug.cgi?id=509326)

<sup>1223</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=513967](https://bugzilla.redhat.com/show_bug.cgi?id=513967)

<sup>1224</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=514485](https://bugzilla.redhat.com/show_bug.cgi?id=514485)

called within a ksh function (defined with the "function" syntax). With this update, referencing the \$! special variable works as expected and the correct process ID of the last background job or function is returned, even when it is referenced from within a ksh script function. (BZ#520383<sup>1225</sup>)

\* when a ksh script included multibyte characters, the ksh script parser sometimes failed to parse the script and printed a syntax error message. This updated package corrects this error: the ksh script parser now correctly handles multibyte characters and no error is returned when they are found. (BZ#538655<sup>1226</sup>)

\* when the built-in ksh typeset function was used with the array variable, it was affecting the size of the array by appending one empty value. This is now corrected and typeset does not unintentionally affect size of arrays. (BZ#538857<sup>1227</sup>)

\* some upstream behavioural changes of ksh were not sufficiently documented, specifically parenthesis which was supported in ksh-93r or older. ksh Now ships Release and ChangeLog documents wherein important changes are documented. (BZ#541654<sup>1228</sup>)

\* when evaluating a non-number variable that contains a point in a numeric comparison, ksh crashed with a segmentation fault. With this update, ksh checks whether the point has numerical or parent separator meaning, and produces only an error message when appropriate. (BZ#548519<sup>1229</sup>)

\* when the array variable was declared using the built-in 'set', but not defined, this declaration did not take effect. The built-in 'set' included in the updated ksh declares array variables correctly. (BZ#553611<sup>1230</sup>)

All users of ksh are advised to upgrade to this updated package, which resolves these issues.

## 1.92. ktune

### 1.92.1. RHBA-2009:1422: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1422](#)<sup>1231</sup>

An updated ktune package that fixes a bug is now available.

The ktune package includes settings for server performance-tuning.

This updated ktune package fixes the following bug:

\* when running a Red Hat Enterprise Linux KVM guest under heavy load, the guest's system clock had the tendency to drift by an amount correlated with the system load. This ktune update provides an

<sup>1225</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=520383](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=520383)

<sup>1226</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=538655](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=538655)

<sup>1227</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=538857](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=538857)

<sup>1228</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=541654](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=541654)

<sup>1229</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=548519](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=548519)

<sup>1230</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=553611](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=553611)



interactive Bourne shell script, `fix_clock_drift.sh`, which, when run as the superuser, inspects various system parameters to determine if the guest on which it is run is susceptible to clock drift under load and, if so, then creates a new "grub.conf.kvm" file in the `/boot/grub/` directory. This file contains a kernel boot line with additional kernel parameters that allow the kernel to account for and prevent significant clock drift on the KVM guest. Note also that the `ntpd` service must be running on the KVM guest for the clock drift to be corrected.

Important: after running `fix_clock_drift.sh` as the superuser, and once the script has created the "grub.conf.kvm" file, then the guest's current "grub.conf" file should be backed up manually by the system administrator, the new "grub.conf.kvm" file should be manually inspected to ensure that it is identical to "grub.conf" with the exception of the additional boot line parameters, the "grub.conf.kvm" file should finally be renamed "grub.conf", and the guest should be rebooted. ([BZ#518039](https://bugzilla.redhat.com/show_bug.cgi?id=518039)<sup>1232</sup>)

Users of Red Hat Enterprise Linux KVM guests that are affected by significant clock drift are advised to upgrade to this updated package, which resolves this issue.

### 1.92.2. RHBA-2010:0238: bug fix and enhancement update

An updated `ktune` package that fixes a clock drift bug in Red Hat Enterprise Linux guests and adds support for the `ktune.d` directory is now available.

The `ktune` package includes settings for server performance-tuning.

This updated `ktune` package fixes the following bug:

\* when running a Red Hat Enterprise Linux KVM guest under heavy load, the guest's system clock had the tendency to drift by an amount correlated with the system load. This `ktune` update provides an interactive Bourne shell script, `fix_clock_drift.sh`, which, when run as with root privileges, inspects various system parameters to determine if the guest on which it is run is susceptible to clock drift under load and, if so, creates a new "grub.conf.kvm" file in the `/boot/grub/` directory. This file contains a kernel boot line with additional kernel parameters that allow the kernel to account for and prevent significant clock drift on the KVM guest. ([BZ#516652](https://bugzilla.redhat.com/show_bug.cgi?id=516652)<sup>1233</sup>)

Note: the `ntpd` service must be running on the KVM guest for the clock drift to be corrected.

Important: this script does not replace the existing `grub.conf` file. If running `fix_clock_drift.sh` creates the file "grub.conf.kvm" the system administrator must set the new file up manually as follows: back up the guest's current "grub.conf" file; inspect "grub.conf.kvm" and ensure it is identical to "grub.conf" with the exception of the additional boot line parameters; re-name "grub.conf.kvm" to "grub.conf"; reboot the guest.

This update also adds the following enhancement:

\* support for `ktune.d` directory has been added to load additional `sysctl` profiles. Each profile could also provide a script for settings which can not be done with `sysctl`. The script will get an option which will be start or stop according to the `ktune` service command used for `ktune`. ([BZ#496940](https://bugzilla.redhat.com/show_bug.cgi?id=496940)<sup>1234</sup>)

Users of Red Hat Enterprise Linux KVM guests, especially those affected by significant clock drift, are advised to upgrade to this updated package, which resolves this issue and adds this enhancement.

---

<sup>1232</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=518039](https://bugzilla.redhat.com/show_bug.cgi?id=518039)

<sup>1233</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=516652](https://bugzilla.redhat.com/show_bug.cgi?id=516652)

<sup>1234</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=496940](https://bugzilla.redhat.com/show_bug.cgi?id=496940)



## 1.93. kudzu

### 1.93.1. RHBA-2010:0191: bug fix and enhancement update

Updated kudzu packages that fix several bugs and add various enhancements are now available.

The updated packages fix the following bugs: - Kudzu would corrupt network configuration information in the presence of some dual and quad-port Chelsio adapters ([BZ#571657](https://bugzilla.redhat.com/show_bug.cgi?id=571657)<sup>1235</sup>) - Kudzu did not properly recognize some USB DVD drives ([BZ#581799](https://bugzilla.redhat.com/show_bug.cgi?id=581799)<sup>1236</sup>)

Also, support for IBM Virtual Fiber Channel devices on the POWER platform has been added. ([BZ#503235](https://bugzilla.redhat.com/show_bug.cgi?id=503235)<sup>1237</sup>)

It is recommended that all users upgrade to the new packages.

## 1.94. kvm

### 1.94.1. RHBA-2009:1423: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1423](https://errata.redhat.com/RHBA-2009:1423)<sup>1238</sup>

Updated kvm packages that resolve an issue are now available.

KVM (for Kernel-based Virtual Machine) is a full virtualization solution for Linux on x86 hardware.

These updated kvm packages fix the following bug:

\* rebooting a KVM guest domain could cause the guest to fail to receive keyboard and mouse input following the reboot. This has been fixed by reinitializing keyboard and mouse state in the guest after it reboots, which resolves the issue. ([BZ#517855](https://bugzilla.redhat.com/show_bug.cgi?id=517855)<sup>1239</sup>)

Note: after installing these updated packages, the following procedure should be carried out to ensure that the fix takes effect:

1. Stop all KVM guest virtual machines (VMs).
2. Either reboot the hypervisor machine, or, as the superuser, remove (using "modprobe -r [module]") and reload (using "modprobe [module]") all of the following modules which are currently running (determined using "lsmod"): kvm, ksm, kvm-intel or kvm-amd.
3. Restart the KVM guest VMs.

All users of kvm are advised to upgrade to these updated packages, which resolve this issue.

<sup>1235</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=571657](https://bugzilla.redhat.com/show_bug.cgi?id=571657)

<sup>1236</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=581799](https://bugzilla.redhat.com/show_bug.cgi?id=581799)

<sup>1237</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=503235](https://bugzilla.redhat.com/show_bug.cgi?id=503235)

<sup>1239</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=517855](https://bugzilla.redhat.com/show_bug.cgi?id=517855)

### 1.94.2. RHBA-2009:1488: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1488](#)<sup>1240</sup>

Updated kvm packages that resolved two issues are now available.

KVM (Kernel-based Virtual Machine) is a full virtualization solution for Linux on x86 hardware. KVM can run multiple virtual machines running unmodified Linux or Windows images. Each virtual machine has private virtualized hardware: a network card, disk, graphics adapter, etc.

These updated packages fix the following bugs:

\* the pthread\_cond\_timedwait time out was not properly handled. Consequently, under some loads, some KVM guests stopped responding to commands from the management interface. (Note: the reproducer was a host running around 300 KVM guests with each guest consuming around 50% of their virtual CPU. On this setup, some guests became non-responsive after several hours.) With this update the time outs are handled properly and KVM guests remain responsive, as expected. ([BZ#526244](#)<sup>1241</sup>)

\* some Linux-based guests that used virtio virtual block devices aborted during installation, returning the error message: "unhandled vm exit: 0x31 vcpu\_id 0".

Using an interface other than virtio for the guest virtual disk was a work around documented in the Red Hat Enterprise Linux 5.4 Technical Notes Known Issues for KVM. The work around was associated with [BZ#518081](#)<sup>1242</sup>, the original Bugzilla report for this issue.

[http://www.redhat.com/docs/en-US/Red\\_Hat\\_Enterprise\\_Linux/5.4/html/Technical\\_Notes/Known\\_Issues-kvm.html](http://www.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/5.4/html/Technical_Notes/Known_Issues-kvm.html)

With this update, the underlying issue (stale EPTP-tagged mappings possibly being used when a virtual CPU or vcpu migrated to a different Physical CPU or pcpu) has been addressed and the work around is no longer necessary: Linux-based guests using virtio virtual block devices no longer abort during installation. ([BZ#527192](#)<sup>1243</sup>)

All users of kvm are advised to upgrade to these updated packages, which resolve this issue.

### 1.94.3. RHBA-2010:0158: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2010:0158](#)<sup>1244</sup>

Updated kvm packages that resolved two issues are now available.

---

<sup>1241</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=526244](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=526244)

<sup>1242</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=518081](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=518081)

<sup>1243</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=527192](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=527192)

KVM (Kernel-based Virtual Machine) is a full virtualization solution for Linux on AMD64 and Intel 64 systems. KVM is a Linux kernel module built for the standard Red Hat Enterprise Linux kernel. KVM can run multiple unmodified, virtualized guest Windows and Linux operating systems.

These updated packages fix the following bug:

\* high loads could cause Microsoft Windows 7 32 bit guests to crash with a Blue Screen error that contained the "HAL\_RTC\_IRQF\_WILL\_NOT\_CLEAR" error code. The updated package resolves this issue and Windows 7 32 bit guests should not crash under high loads.

All KVM users should upgrade to these updated packages, which contain backported patches to resolve these issues. Note that the procedure in the Solution section must be performed before this update takes effect.

### 1.94.4. RHSA-2010:0271: Important security, bug fix and enhancement update

Updated kvm packages that fix one security issue, multiple bugs, and add enhancements are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

KVM (Kernel-based Virtual Machine) is a full virtualization solution for Linux on AMD64 and Intel 64 systems. KVM is a Linux kernel module built for the standard Red Hat Enterprise Linux kernel.

A flaw was found in the way QEMU-KVM handled erroneous data provided by the Linux virtio-net driver, used by guest operating systems. Due to a deficiency in the TSO (TCP segment offloading) implementation, a guest's virtio-net driver would transmit improper data to a certain QEMU-KVM process on the host, causing the guest to crash. A remote attacker could use this flaw to send specially-crafted data to a target guest system, causing that guest to crash. ([CVE-2010-0741](#)<sup>1245</sup>)

- Setting the `cpu_set` variable to **1 online** in the **qemu Monitor** and then shutting down the guest would cause the host or the guest to crash. The updated package resolves this issue and prevents the host or guest from crashing in this scenario. ([BZ#487857](#)<sup>1246</sup>)
- The KVM configure script would not abort if the correct options were not enabled. The KVM configure script now verifies features are enabled or disabled by the configure script and aborts if the features was not loaded as requested. ([BZ#489900](#)<sup>1247</sup>)
- The para-virtualized network drivers (**virtio-net**) lacked non-maskable interrupt (NMI) injection masking on AMD-based hosts. This caused Windows XP guests using the para-virtualized network driver could fail with a Blue Screen error during certain tests. The updated packages resolve this issue. ([BZ#492290](#)<sup>1248</sup>)
- Timer events were processed before entering guest mode. This meant that certain timer events may not have been processed. Timer events are now processed in the main VCPU event loop so timer events are processed while the VCPU is halted. Timer events may inject interrupts or non-maskable interrupt (NMI) which will then un halt the VCPU. This fixes the issue of unconditionally un halting the VCPU. ([BZ#492663](#)<sup>1249</sup>)

<sup>1245</sup> <https://www.redhat.com/security/data/cve/CVE-2010-0741.html>

- If one or more VCPUs was disabled, VCPUs would appear in Windows Server 2008 **Device Manager** as devices with the ! symbol indicating an error. Windows does not handle CPUs marked as present (bit 0 in ACPI spec), but not enabled (bit 1), which causes this issue.

However, there are situations where Linux expects CPUs to be present but not enabled. This is a heuristic test used by Linux to determine if a CPU is hot-pluggable.

The updated package fixes virtualized CPU detection for Windows but breaks the ability to hot-add CPUs into Linux guests. ([BZ#495844](#)<sup>1250</sup>)

- Using the numeric keypad of a keyboard with or without **Num Lock** produced erroneous input on guests accessed with VNC through the QEMU monitor application. The number pad keys should now work for input on guests accessed with VNC. ([BZ#497507](#)<sup>1251</sup>)
- An unhandled interrupt from the `kvm_vcpu_block()` call unhalting a VCPU outside of the interrupt window. As a consequence, when the "**there is no bootable disk**" error presented the `qemu` process used 100% of the available CPUs. The updated packages resolve this issue and the interrupt is now handled correctly. ([BZ#502086](#)<sup>1252</sup>)
- Windows Server 2008 R2 guests would hang after a restart if the guest was created with multiple VCPUs. This was caused by not properly filtering non-maskable interrupts (NMIs) from the guests during the restart procedure. The updated packages fix this issue and Windows Server 2008 R2 guests can successfully use multiple VCPU. ([BZ#502543](#)<sup>1253</sup> [BZ#503322](#)<sup>1254</sup>)
- Migrating a paused guest caused the guest to resume at the destination. Paused guests now remain paused after a migration. ([BZ#503367](#)<sup>1255</sup>)
- Multiple virtualized guests using the hypercall device resulted in one or more of the guests using 100% of their assigned CPUs or becoming unresponsive. The updated packages fix the hypercall device, preventing this issue. ([BZ#503759](#)<sup>1256</sup>)
- VCPUs were not reported correctly to Windows XP guests. On the Windows XP guest the number for CPUs listed in **Task Manager** was lower than the number of CPUs assigned to the guest. Windows XP guests should now use and display the number of VCPUs assigned if the guest can handle that number of CPUs. ([BZ#508040](#)<sup>1257</sup>)
- A segmentation fault occurred when a guest used a `i82551` emulated network interface card was used. The segmentation fault is fixed in the packages. ([BZ#510706](#)<sup>1258</sup>)
- Creating guests that use both 64k and 4k image block cluster sizes and virtualized IDE as the storage device driver would cause a segmentation fault in the `qemu-kvm` process. The updated packages resolve this issue. ([BZ#542923](#)<sup>1259</sup>)
- Running the `migrate_set_speed` command in the QEMU console after running `migrate_cancel` causes segmentation fault in KVM. The updated packages fix this issue and the code causing the segmentation fault is fixed. ([BZ#522887](#)<sup>1260</sup>)
- A segmentation fault occurred when using the `qemu-img rebase` command to rebase an image snapshot. ([BZ#563141](#)<sup>1261</sup>)
- The `qemu-img rebase` command failed with an "Operation not supported" error message when it was run on locally-attached block devices. ([BZ#569762](#)<sup>1262</sup>)

- The **qemu-img** command failed to copy a RAW image to a Fibre Channel storage device. The **qemu-image** command can now copy, convert and create images on Fibre Channel storage devices. ([BZ#511072](#)<sup>1263</sup>)
- Storage I/O errors were processed out of order causing the guest to change state or crash unexpectedly. The guest state handlers now process storage I/O errors in the proper order. ([BZ#514522](#)<sup>1264</sup>)
- A guest would occasionally not accept keystrokes or mouse clicks after rebooting. The updated package resolves this issue and user interactions are accepted after repeatedly rebooting guests. ([BZ#515275](#)<sup>1265</sup>)
- In rare instances, certain virtualized guests could lock up while requesting a **raw\_pread** system call. The offset was larger than the file size of the read failures which causes the system to infinitely loop I/O requests. This could, in certain circumstances lead to file system corruption on virtualized guests. The updated packages add a result test which prevents the infinite request loop. ([BZ#515655](#)<sup>1266</sup>)
- The guest could change the QXL device ROM which could result in memory corruption. The updated packages prevent the guest from modifying the QXL device ROM. ([BZ#537888](#)<sup>1267</sup>)
- The MRS storage array (msr's) in **kvm\_arch\_save\_regs()** function. The array was sized too small for the function and may cause stack corruption. ([BZ#528917](#)<sup>1268</sup>)
- Incorrectly handled I/O errors could cause guests file system corruption when using the para-virtualized block drivers and IDE emulation of NFS storage. The updated packages resolve this issue and host I/O errors will pause the guest instead of causing file system corruption. ([BZ#531827](#)<sup>1269</sup>)
- With Red Hat Enterprise Virtualization, the **virtio\_blk\_dma\_restart\_bh()** function previously handled write errors. The function was not updated for this, causing read errors to be resubmitted as writes. This caused guest image corruption in some cases.

Additionally, the return values of the **bdrv\_aio\_write()** and **bdrv\_aio\_read()** functions were ignored. If an immediate failure occurred in one of these functions, errors would be missed and the guest could hang or read corrupted data. ([BZ#552487](#)<sup>1270</sup>)

- with Red Hat Enterprise Virtualization, guests continued to run after encountering disk read errors. This could have caused guest file systems to corrupt (but not the host's), notably in environments that use networked storage. With this update, the **qemu-kvm** command's **-drive "werror=stop"** option now applies not only to write errors but also to read errors. When using this option, guests will pause on disk read and write errors.

By default, guests managed by Red Hat Enterprise Virtualization use the **"werror=stop"** option. This option is not used by default for guests managed by libvirt. ([BZ#533390](#)<sup>1271</sup>)

- KVM would crash or fail to boot when attempting to assign 64GB of memory to 32-bit guests using PAE. KVM now supports addressing up to 48 bits of physical memory with PAE. ([BZ#516545](#)<sup>1272</sup>)
- Windows Server 2003 32-bit guests assigned more than 4GB of RAM would crash after rebooting the guest. The updated packages resolve this issue and Windows Server 2003 32-bit guests can be assigned more than 4GB of RAM. 32-bit guests may not be able to use more than 4GB of RAM, refer to the guest operating system's documentation. ([BZ#516762](#)<sup>1273</sup>)

- 64-bit guests would hang on an AMD host if one or more of the guest's VCPUs were changed from offline to online. This issue is resolved in the updated package. ([BZ#525699](#)<sup>1274</sup> and [BZ#517223](#)<sup>1275</sup>)
- When using the virtual vm8086 mode, bugs in the emulated hardware task switching implementation may have caused older guest operating systems to malfunction. ([BZ#517324](#)<sup>1276</sup>)
- An **"unhandled vm exit: 0x31 vcpu\_id 0"** error message could appear when installing certain guest operating systems, such as SUSE Linux Enterprise Server 11, using a para-virtualized block device (virtio-blk). The updated packages resolve this issue and installation with the para-virtualized drivers is supported and working. ([BZ#518081](#)<sup>1277</sup>)
- The `__kvm_mmu_free_some_pages` list was not verified empty before it was used. The updated package verifies the `__kvm_mmu_free_some_pages` list is empty before attempting to look at list entries. ([BZ#519397](#)<sup>1278</sup>)
- Windows Server 2008 64 bit guests use a **cr8** call which executed a **vmexit** call. This caused performance issues for Windows Server 2008 guests. The updated packages use a different call method to handle **cr8** calls which significantly improves the performance of Windows Server 2008 64 bit guests. ([BZ#520285](#)<sup>1279</sup>)
- When attempting to resume from hibernate with Windows Server 2003 guests, KVM would attempt to stop the QEMU emulated audio device which was not activated. This caused a **"snd\_playback\_stop: ASSERT playback\_channel->base.active failed"** error message to appear and the resume process to fail and the guest to crash. The updated package resolves this issue. ([BZ#520394](#)<sup>1280</sup>)
- Time drift may have occurred in Windows guests that use the IOAPIC interrupt for timing. The updated packages resolve this issue and Windows guests should now keep time accurately. ([BZ#521025](#)<sup>1281</sup>)
- Windows Server 2003 (32-bit and 64-bit) guests may have experienced time drift. ([BZ#543137](#)<sup>1282</sup>)
- On AMD hosts, Window Server 2008 R2 Datacenter guests would stop during the installation at the step **"Setup will continue after restarting your computer"**. This issue is resolved and Windows Server 2008 R2 Datacenter guests now successfully install. ([BZ#521749](#)<sup>1283</sup>)
- Resetting the PCI status of a para-virtualized network device (virtio-net) would cause KVM to crash. This issue is resolved the the updated packages. ([BZ#521829](#)<sup>1284</sup>)
- The German keyboard map was missing some keys in when accessing a guest with VNC. The German keyboard map now contains all keys when accessing guests with VNC. ([BZ#521835](#)<sup>1285</sup>)
- When a guest issued an Inter-processor Interrupt (IPI) call, the call would cause KVM to issue a global IPI call on the host. The global IPI call interrupts all processors instead of just those assigned to the guest. The updated packages resolve the issue by using the kernel's IPI handling functions instead of emulating the IPI handler. ([BZ#524970](#)<sup>1286</sup>)
- KVM and virtualized guests would become unresponsive due to waiting infinitely for an a.io threads to return. The updated packages resolve this issue by correctly timing out threads which do not return. ([BZ#525114](#)<sup>1287</sup>)
- The host KVM process could crash or use 100% of the allocated CPUs when a guest with more than one VCPU received high volumes of network traffic through a device using the para-virtualized network drivers (virtio-net). This issue is resolved in the updated packages. ([BZ#525323](#)<sup>1288</sup>)



- KVM did not change the package address of the **etherboot.zrom** file. KVM would always use the default, the **ne.zrom** file. Guests could not get an IP address or access PXE servers. The updated packages resolve this issue and guests can access PXE server when using non-default network devices. ([BZ#526124](#)<sup>1289</sup>)
- KVM could generate invalid memory types in Memory Type Range Registers (MTRR) and Page Attribute Tables (PAT). This could be used by guests running random code to possibly store (and later use) a random MTRR type. The updated package prevents these invalid memory types from being created. ([BZ#526837](#)<sup>1290</sup>)
- An error in the Makefile prevented users from using the source RPM to install KVM. ([BZ#527722](#)<sup>1291</sup>)
- Linux guest **initrd** images greater than 4GB would cause the guest to crash. KVM now limits the size of **initrd** images to less than 4GB. ([BZ#529694](#)<sup>1292</sup>)
- If the **qemu-kvm** command's `-net user` option was used, unattended Windows XP installations would not receive an IP address after rebooting. The guest requests a second DHCP address which makes the list of free DHCP addresses run out much quicker. This issue is fixed by reassigning the same address requested with DHCP to the guest after the guest reboots. ([BZ#531631](#)<sup>1293</sup>)
- The para-virtualized clock (pvclock) Mode-specific register values were not preserved after a migration. This issue also affected the para-virtualized clock when a guest was saved and restored. These drivers not being saved could cause the guest's time keeping to become significantly skewed after restoring or migrating the guest. In the updated packages, the MSR values are preserved when a guest is saved and restored, and for migrations. ([BZ#531701](#)<sup>1294</sup>)
- Installing Windows Server 2008 R2 from an ISO image could result in a blue screen "BAD\_POOL\_HEADER" stop error. ([BZ#531887](#)<sup>1295</sup>)
- Running certain test functions on Windows 7 guests caused a blue screen "HAL\_RTC\_IRQF\_WILL\_NOT\_CLEAR" stop error. ([BZ#556455](#)<sup>1296</sup>)
- Windows Server 2003 R2 Service Pack 2 32-bit guests using the para-virtualized block drivers could crash with an **unhandledvm exit** error during reboot. The hypervisor now handles this error, resolving the issue. ([BZ#532086](#)<sup>1297</sup>)
- After restoring a migrated Windows Server 2008 R2 guest, a race condition caused the guest to hang during the shut down sequence. The updated packages resolve this issue and Windows Server 2008 R2 guests will successfully shut down when requested after a migration. ([BZ#533090](#)<sup>1298</sup>)
- a bug in the **grow\_refcount\_table()** error handling caused infinite recursion in some cases. This caused the **qemu-kvm** process to hang and eventually crash. ([BZ#537075](#)<sup>1299</sup>)
- Full I/O error codes were not passed up to the host or the Red Hat Enterprise Virtualization Manager. Accurate I/O error codes are now forwarded to the user and management tools. ([BZ#537077](#)<sup>1300</sup>)
- There was a regression in the **qemu-img** command, Fibre Channel devices could not be formatted using RAW or use preallocated RAW devices. The **qemu-img** command is updated to handle Fibre Channel devices in the RAW format. ([BZ#537655](#)<sup>1301</sup>)

- Guests could not eject CD-ROMs from physical CD-ROM drives attached to the guest. The updated packages resolve this issue and guests can now eject CD-ROMs from physical CD-ROM drives. ([BZ#539250](#)<sup>1302</sup>)
- The qcow2 file format unnecessarily rounded up the length of the backing format string to the next multiple of 8. The array in `BLOCKDRIVERSTATE` can only store 15 characters, causing backing formats with 9 characters or more to fail. This issue affected devices using the `host_device` format. The updated packages resolve this issue by determining the length of the backing format of qcow2 devices. ([BZ#540893](#)<sup>1303</sup>)
- Migrations could fail due to invisible physical CPU states. A new set of IOCTL exports report user-invisible states related to exceptions, interrupts, and Non-Maskable Interrupts (NMIs). These functions allow management tools to prevent this type of failed migration. ([BZ#541084](#)<sup>1304</sup>)
- Guests could not PXE boot with gPXE and an emulated e1000 network interface card. The updated packages fix this issue and guests can boot images using gPXE and the emulated e1000 driver. ([BZ#543979](#)<sup>1305</sup> and [BZ#550265](#)<sup>1306</sup>)
- The KVM process could become non-responsive if a networked or local connect to the QXL driver was lost while the driver was running. This cause a "**qxl\_display\_update: waiting for command**" error message to be printed in the logs. The updated packages resolve this issue. ([BZ#544785](#)<sup>1307</sup>)
- The `qemu-kvm` man page incorrectly described the qcow2 default as `cache=writeback`. The default is `cache=none` for qcow2 images and `cache=writethrough` for all other disk types. The man page for `qemu-kvm` has been updated to reflect this. ([BZ#545194](#)<sup>1308</sup>)
- KVM did not verify if barriers were required for migration. KVM now verifies if barriers are required for guest migration and disables barriers if they are not required. ([BZ#549938](#)<sup>1309</sup>)
- The hypercall driver for Windows guests did not reset the device when the guest was shut down or rebooted. This occasionally caused the driver to use 100% of the CPU and cause the guest to hang. ([BZ#550755](#)<sup>1310</sup>)
- The `kvm-qemu-img` command failed to convert sparse RAW image files to qcow2 sparse snapshot image files. ([BZ#558195](#)<sup>1311</sup>)
- Migration with the `-M rhe15.5.0` parameter did not work for migration to or from Red Hat Enterprise Linux 5.5. Migration with the `-M` parameter is now supported and functional. ([BZ#559163](#)<sup>1312</sup>)
- Removed a warning message which appeared when the `-initrd` option was used. ([BZ#512672](#)<sup>1313</sup>)
- The KVM kernel module would panic if the `paging64_sync_page()` call was executed on a system using PCI passthrough devices. This kernel panic error could occur if a guest with an attached PCI device was started. The updated packages resolve this issue. ([BZ#566385](#)<sup>1314</sup>)
- Various issues with compiling the KVM modules and packages. ([BZ#533453](#)<sup>1315</sup>, [BZ#533059](#)<sup>1316</sup>, [BZ#539589](#)<sup>1317</sup> and [BZ#533197](#)<sup>1318</sup>)
- Removed a debugging message `qemu_popen: returning result of qemu_fopen_ops` that displayed when saving a virtualized guest state into a compressed file. ([BZ#530533](#)<sup>1319</sup>)



These updated packages add the following enhancements:

- Support for migration and image compatibility between Red Hat Enterprise Linux 5.4.4 and Red Hat Enterprise Linux 5.5 hosts. ([BZ#553187](#)<sup>1320</sup> and [BZ#557327](#)<sup>1321</sup>)
- The KVM hypervisor does not accept **MSR\_KERNEL\_GS\_BASE** intercept calls for Windows Server 2008 guests. This improves performance of Windows Server 2008 guests under heavy loads. ([BZ#488130](#)<sup>1322</sup>)
- qcow2 now uses 64Kb as the default block cluster size instead of 4Kb blocks which improves performance for guests using qcow2. ([BZ#502809](#)<sup>1323</sup>)
- Various unsupported features of the **qemu-kvm** command are now compiled out of the kvm packages. ([BZ#516672](#)<sup>1324</sup>)
- Support for migration from older hypervisors which use versions of savevm with additional fields which are not supported by newer versions. This feature is required for migrations from older hypervisors to newer versions of KVM. ([BZ#541731](#)<sup>1325</sup>)
- Significantly improved performance of qcow2 devices using the *cache=off* parameter. ([BZ#518169](#)<sup>1326</sup>)
- Support for guest access to advanced CPU extensions, including: SSE4.1, SSE4.2 and SSE4a. ([BZ#518090](#)<sup>1327</sup>)
- SMBIOS table 4 data is now generated for Windows guests. ([BZ#537178](#)<sup>1328</sup>)
- The cache flushing command was changed from **fsync** to **fdatasync**. This allows write caches to be exposed to guests and allows the guest to request for flushing I/O buffers. This improves I/O performance for some guests. ([BZ#537646](#)<sup>1329</sup>)
- KVM can now use gPXE or **etherboot** roms stored in the **/usr/share/qemu-pxe-roms** directory. ([BZ#546019](#)<sup>1330</sup> and [BZ#550053](#)<sup>1331</sup>)
- Support for changing the file format of an in-place backing file. ([BZ#530134](#)<sup>1332</sup>)
- Support for Red Hat Enterprise Linux 3.9 guests running the para-virtualized drivers. ([BZ#536749](#)<sup>1333</sup>)
- The QXL driver now supports setting resolutions of 1024x576 and 1024x600. ([BZ#552240](#)<sup>1334</sup>)

All KVM users should upgrade to these updated packages, which resolve this issue as well as fixing the bugs and adding the enhancements noted in the Technical Notes. Note: The procedure in the Solution section must be performed before this update will take effect.

## 1.95. less

### 1.95.1. RHBA-2010:0214: bug fix and enhancement update

A re-based less package that also fixes two bugs is now available.

The less utility is a text file browser that resembles more, but with more capabilities ("less is more"). The less utility allows users to move backwards in the file as well as forwards. Because less need not read the entire input file before it starts, less starts up more quickly than text editors (vi, for example).

This update re-bases less from version 394 to version 436. Notes regarding the changes introduced by this re-base can be found at the upstream release notes links listed in the References field below.

This update also addresses to specific issues as follows:

\* a previous less update, released as RHBA-2009-0413 and addressing

[BZ#441691](#)<sup>1335</sup>, introduced a regression: when scrolling line-by-line, some lines were truncated and some lines were duplicated. This update corrects the regression and scrolling line-by-line through a file now displays text as expected. ([BZ#509553](#)<sup>1336</sup>)

\* the "--old-bot" switch (a switch which forces less to revert to its original bottom of screen behavior when scrolling forward through a file) was not documented in the less man page. This update adds appropriate documentation of this switch. ([BZ#510724](#)<sup>1337</sup>)

All less users should upgrade to this re-based package, which resolves these issues.

## 1.96. libXi

### 1.96.1. RHBA-2010:0127: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2010:0127](#)<sup>1338</sup>

Updated libXi packages that resolve an issue are now available.

libXi is the X.Org XInput runtime library.

These updated libXi packages fix the following bug::

\* the XInitThreads() function initializes Xlib support for concurrent threads. Calling the XInitThreads() function could have caused deadlock with the result that the calling program became unresponsive. With this update, programs which call XInitThreads() in the correct manner do not suffer from deadlock and do not hang, thus resolving the issue. ([BZ#563120](#)<sup>1339</sup>)

All users of libXi are advised to upgrade to these updated packages, which resolve this issue.

---

<sup>1335</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=441691](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=441691)

<sup>1336</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=509553](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=509553)

<sup>1337</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=510724](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=510724)

<sup>1339</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=563120](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=563120)

## 1.97. libXrandr

### 1.97.1. RHBA-2009:1608: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2009:1608](#)<sup>1340</sup>

An updated libXrandr package that fixes a dependency bug is now available.

libXrandr is the runtime library for the X11 RandR extension.

This update addresses the following issue:

\* the libXrandr-devel package requires libXext-devel to work but the package's spec file was missing the necessary "Requires" line. If libXrandr-devel was installed separately (for example, by running "yum install libXrandr-devel") and libXext-devel was not already installed, libXrandr-devel did not work. This dependency has been added to the spec file with this update: installing the libXrandr-devel package now pulls down all required dependencies, ensuring libXrandr-devel works as expected. ([BZ#498044](#)<sup>1341</sup>)

Users are advised to upgrade to this updated libXrandr package, which resolves this problem.

## 1.98. libXt

### 1.98.1. RHBA-2010:0192: bug fix update

An updated libXt package that fixes a bug which prevented C++ code from building is now available.

libXt is the X toolkit intrinsics runtime library.

\* conflicting declarations in several header files meant C++ code could not be compiled against libXt. With this update, these conflicts have been resolved and C++ applications can, once again, build against the libXt library. ([BZ#487354](#)<sup>1342</sup>)

Users are advised to upgrade to this updated package, which resolve this problem.

## 1.99. libaio

### 1.99.1. RHBA-2010:0277: bug fix update

An enhanced libaio package is now available.

The Linux-native asynchronous I/O facility ("async I/O" or "aio") has a richer API and capability set than the simple POSIX asynchronous I/O facility. This library, libaio, provides the Linux-native API

<sup>1341</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=498044](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=498044)

<sup>1342</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=487354](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=487354)

for asynchronous I/O. The POSIX asynchronous I/O facility requires this library in order to provide kernel-accelerated asynchronous I/O capabilities, as do applications which require the Linux-native asynchronous I/O API.

Red Hat Enterprise Linux lacked support for `eventfd`, which generates file descriptors. These descriptors are used to provide an event wait/notify mechanism for userspace applications. `eventfd` has now been added to the API and integrated with Asynchronous Input/Output (AIO). It eliminates the need to use pipes to signal events, reducing kernel overhead as it does not consume two file descriptors each time, as the previous method did. `eventfd` also offers an `fd-bridge` and can be used to signal the readiness of interfaces that would otherwise be incompatible with the Linux kernel. ([BZ#540626](#)<sup>1343</sup>)

Users are advised to upgrade to this updated `libaio` package, which adds this enhanced functionality. [Kernel update needed: RHBA-2009:9260]

## 1.100. `libcmptutil`

### 1.100.1. RHBA-2010:0222: bug fix and enhancement update

An updated `libcmptutil` package that fixes bugs and introduces feature enhancements is now available.

`libcmptutil` provides a convenient API for performing common tasks with different CMPI providers.

\* the `libcmptutil` package is used by the `libvirt-cim` package. An update to the `libvirt-cim` package requires this update. ([BZ#540843](#)<sup>1344</sup>)

Users are advised to upgrade to this updated `libcmptutil` package, which resolves these issues and adds these enhancements.

## 1.101. `libevent`

### 1.101.1. RHEA-2010:0244: enhancement update

An updated `libevent` package that rebases to the current stable upstream release is now available.

The `libevent` API provides a mechanism to execute a callback function when a specific event occurs on a file descriptor or after a timeout has been reached. `libevent` is meant to replace the asynchronous event loop found in event driven network servers. An application just needs to call `event_dispatch()` and can then add or remove events dynamically without having to change the event loop.

This update rebases the `libevent` library included with Red Hat Enterprise Linux from version 1.1a to the current stable upstream release, version 1.4.13. ([BZ#476557](#)<sup>1345</sup>)

For details on the changes between these two versions see the upstream Changelogs available on the `libevent` home page:

<http://monkey.org/~provos/libevent/>

---

<sup>1343</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=540626](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=540626)

<sup>1344</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=540843](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=540843)

<sup>1345</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=476557](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=476557)

All users of libevent or applications that use the libevent library should install this updated package.

## 1.102. libgnomecups

### 1.102.1. RHBA-2009:1577: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2009:1577](#)<sup>1346</sup>

Updated libgnomecups packages that resolve an issue are now available.

The libgnomecups library integrates CUPS (the Common Unix Printing System) with the GNOME desktop

These updated libgnomecups packages fix the following bug:

\* previously, the .lpoptions file in the user's home directory contained the default user-specific print queue options. For CUPS version 1.2, this file changed locations to the ~/.cups/lpoptions file. These updated packages make libgnomecups aware that the new location for user-specific print queue options is the ~/.cups/lpoptions file. ([BZ#509064](#)<sup>1347</sup>)

All CUPS users are advised to upgrade to these updated packages, which resolve this issue.

## 1.103. libgtop2

### 1.103.1. RHBA-2010:0099: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2010:0099](#)<sup>1348</sup>

Updated libgtop2 packages that resolve an issue are now available.

The libgtop2 package contains a library that enables access to information related to system statistics such as CPU, memory and disk usage, active processes, PIDs, and more.

These updated libgtop2 packages fix the following bug:

\* stat files live under the /sys/block directory; for example, /sys/block/sda/sda1/stat would be the stat file corresponding to the first partition on the first (non-IDE) drive. These stat files provide several statistics about the state of a block device. However, libgtop2 parsed the line of information supplied by stat files on recent versions of Red Hat Enterprise Linux incorrectly, which caused, for example,

<sup>1347</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=509064](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=509064)

the GNOME System Monitor utility to display graphs which used incorrect colors and/or values. This update ensures that the stat files are parsed correctly and thus supply correct information to applications which make use of libgtop2. ([BZ#548693](https://bugzilla.redhat.com/show_bug.cgi?id=548693)<sup>1349</sup>)

\* libgtop2 was unable to correctly parse /proc/[pid]/smaps files to determine memory usage information due to the fact that a field for swap usage was added to smaps files. This update fixes the parser so that it is once again able to correctly parse smaps files. ([BZ#562817](https://bugzilla.redhat.com/show_bug.cgi?id=562817)<sup>1350</sup>)

All users are advised to upgrade to these updated packages, which resolve this issue.

## 1.104. libhugetlbfs

### 1.104.1. RHEA-2010:0056: enhancement update



#### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHEA-2010:0056](https://errata.redhat.com/RHEA-2010:0056)<sup>1351</sup>

An updated libhugetlbfs package that adds a script to simplify huge page setup is now available.

The libhugetlbfs library interacts with the Linux hugetlbfs to make large pages available to applications in a transparent manner.

This update adds the following enhancement.

\* previously, huge pages worked well once configured but setting them up was a complicated, multi-step, potentially error-prone process. This updated package includes a script -- `huge_page_setup_helper` -- that asks for three pieces of data and then sets up huge pages for use based on the answers provided. The three data points required by the script are the memory to allocate to huge pages and the group and users who should be allowed access to the huge pages. ([BZ#523346](https://bugzilla.redhat.com/show_bug.cgi?id=523346)<sup>1352</sup>)

All huge pages users should install this updated package which includes this enhancement.

## 1.105. libsepol

### 1.105.1. RHBA-2010:0183: bug fix update

An updated libsepol package that resolves a policy issue is now available.

libsepol provides an API for the manipulation of SELinux binary policies. It is used by checkpolicy (the policy compiler) and similar tools, and programs such as `load_policy`, which must perform specific transformations on binary policies (for example, customizing policy boolean settings).

This updated libsepol package addresses the following issue:

---

<sup>1349</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=548693](https://bugzilla.redhat.com/show_bug.cgi?id=548693)

<sup>1350</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=562817](https://bugzilla.redhat.com/show_bug.cgi?id=562817)

<sup>1352</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=523346](https://bugzilla.redhat.com/show_bug.cgi?id=523346)

\* newer SELinux kernels have access checks that the shipping SELinux policy package does not understand. The kernel currently denies these access checks by default. This updated libsepol package allows the checkpolicy and selinux-policy packages to build policy that tells the kernel to "Allow" unknown access. ([BZ#531228](#)<sup>1353</sup>)

All SELinux users should install this updated package which resolves this issue.

## 1.106. libuser

### 1.106.1. RHBA-2009:1525: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1525](#)<sup>1354</sup>

Updated libuser packages that fix a bug are now available.

The libuser library implements a standardized interface for manipulating and administering user and group accounts. Applications that are modeled after applications from the shadow password suite are included in these packages.

These updated libuser packages fix the following bug:

\* nscd, the name service caching daemon, provides a cache for common name service requests. The libuser utilities were unable to signal to nscd that its cache should be refreshed, which caused name service delays after changing user account information. For example, after adding a new user with the useradd utility, the newly-added user was not available until nscd invalidated and subsequently rebuilt its cache. With this update, the libuser utilities are once again able to signal to nscd that it should rebuild its cache, with the effect that changes that affect the name service take effect more quickly. ([BZ#528644](#)<sup>1355</sup>)

All users of libuser are advised to upgrade to these updated packages, which resolve this issue.

## 1.107. libvirt

### 1.107.1. RHBA-2009:1424: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1424](#)<sup>1356</sup>

Updated libvirt packages that resolve an issue are now available.

<sup>1353</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=531228](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=531228)

<sup>1355</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=528644](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=528644)



The libvirt library is a C API for managing and interacting with the virtualization capabilities of Linux and other operating systems. In addition, libvirt provides tools for remotely managing virtualized systems.

These updated libvirt packages fix the following bug:

\* the PIT clock is the programmable interrupt timer clock, which triggers interrupts at certain counts, and is the default clock for Red Hat Enterprise Linux KVM guests. Guests which used the PIT experienced clock drift due to interrupt re-injection. The "-no-kvm-pit-reinject" option has now been added to the KVM command line, which solves potential clock drift on Red Hat Enterprise Linux KVM guests. ([BZ#517903](#)<sup>1357</sup>)

All libvirt users are advised to upgrade to these updated packages, which resolve this issue.

### 1.107.2. RHBA-2010:0205: bug fix and enhancement update

Updated **libvirt** packages that fix several bugs and introduce feature enhancements are now available for Red Hat Enterprise Linux 5.

These updated packages fix the following bugs:

- On Xen guests, the netfront and RTL8192 network drivers could run concurrently, bringing up two network interfaces where only one was configured. The two interfaces would share the same MAC address and could cause networking difficulties. Support for a netfront interface model has been added, meaning only the single netfront interface is configured.

[BZ#483884](#)<sup>1358</sup>

- The storage pool deletion routine did not distinguish between files and directories when removing data. As a result, inactive storage pools could not be deleted. With this update, files and directories are removed appropriately, allowing inactive storage pools to be deleted.

[BZ#496579](#)<sup>1359</sup>

- When adding a new physical host PCI device, **libvirt** would not attempt to reset the PCI bus if other functions or devices were present on the same bus. Some PCI devices could not be utilized for virtualization as a result. Attempts to reset the PCI bus will now be made, allowing affected devices to be used for virtualization.

[BZ#500213](#)<sup>1360</sup>

- Devices attached to a guest in managed mode were not automatically re-attached to the host OS when the guest shut down. Manual intervention was required to use these devices again when the guest is re-started. Managed mode devices will now be re-attached to the host when the guest shuts down, allowing them to be automatically used when the guest is re-started..

[BZ#500217](#)<sup>1361</sup>

- The Xen driver was not checking that guest domains with the same UUID also had the same name. Using the **virsh edit** command to change the name of a Xen domain would make a new copy of the configuration file with the new name, but not alter the original configuration file. UUIDs and names for guest domains are now checked to ensure they match. Attempting to change the name

---

<sup>1357</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=517903](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=517903)

of a domain using the **virsh edit** command will now return an error message and not make any change to the system.

[BZ#504262](#)<sup>1362</sup>

- Valid values for the credit scheduler parameter are in the range *0-65534*. A value of *65535* was being accepted as valid, but would not alter the scheduler configuration. With this release, only values within the valid range are accepted.

[BZ#504914](#)<sup>1363</sup>

- Using the **info** command to change memory values on a KVM guest showed that inactive KVM guest memory was not being reported correctly. Memory reporting for unused domains was corrected in the **qemu** driver and the info command now returns the correct value.

[BZ#508266](#)<sup>1364</sup>

- Running the command **virsh vol-key volname** was sometimes resulting in a segmentation fault. A change was made to the way pool objects are handled and the key lookup no longer crashes.

[BZ#509293](#)<sup>1365</sup>

- Using the pool parameter with the **virsh vol-path** command would result in errors. The **virsh vol-path** command was altered to support the pool parameter and the errors no longer occur.

[BZ#509306](#)<sup>1366</sup>

- The **virsh find-storage-pool-sources** command failed to find any **dir/nfs/netfs** pool sources and failed with **unknown failure**. The error reporting was fixed and the command now works as expected.

[BZ#509979](#)<sup>1367</sup>

- The **virsh nodedev-create** command resulted in an out of memory error. This was found to be a false positive. The checks were updated, and the error now only occurs if there is an actual memory problem.

[BZ#510426](#)<sup>1368</sup>

- Two different methods were using the same name for different **libvirt** entry points, which created a device error when creating nodes. One of the methods was renamed and node creation now works as expected.

[BZ#510427](#)<sup>1369</sup>

- Running the **virsh nodedev-destroy** command to destroy a NIC interface caused **libvirtd** to hang indefinitely. The locking issue was found and rectified and the **libvirtd** crash no longer occurs.

[BZ#510430](#)<sup>1370</sup>

- Running the **virsh vol-delete** command produced a **failed to connect to the hypervisor** error and **libvirtd** needed to be restarted. The code was altered to refresh

allocation and permissions information, but not capacity information, and the command now works as expected.

[BZ#510450](#)<sup>1371</sup>

- When an XML configuration file was generated using **virsh dumpxml** for a running virtual machine, it contained parameters used for backwards compatibility with previous versions. **virt-xml-validate** would report that the generated file was not valid because of these legacy parameters. The validate program was altered to accept the parameters used in the generated XML file, which now validates correctly.

[BZ#512069](#)<sup>1372</sup>

- Running concurrent TLS connections under the **libvirt** python wrapper caused **libvirt** to crash. Changes were made to the way that **GNUTLS** handles threading and the crash no longer occurs.

[BZ#512367](#)<sup>1373</sup>

- **libvirt** was not reporting current vCPU and pCPU placement or the vCPU execution time counter accurately. The behavior was changed so that **libvirt** doesn't find out the affinity when set with **taskset**, but does when set with **virsh vcpupin**. The reporting is now correct.

[BZ#514082](#)<sup>1374</sup>

- Creating npiv devices works as expected, but puts error messages into the **/var/log/messages** file. The Opened WWN path **/sys/class/fc\_host//host5/port\_name** for reading message was updated and the error messages no longer appear in the log file.

[BZ#514324](#)<sup>1375</sup>

- The **virsh** man page described “most operations” as being asynchronous, which is not the case. The man page was updated to state that most operations are synchronous except creation and shutdown of domains.

[BZ#514532](#)<sup>1376</sup>

- Guests that use the default source clock try to compensate for lost ticks by reading the TSC as well. This can cause the guest clock to go out of synchronization. All Red Hat Enterprise Linux guests now unconditionally add **--no-kvm-pit-reinjection** to the **qemu** command line, and the guest no longer falls out of synchronization.

[BZ#517278](#)<sup>1377</sup>

- **libvirt** would not perform a power management reset if there were other functions on the device. The PCI Power Management reset only affects individual functions, and not the whole device. The check for other functions was removed, so that where both are available, the whole device reset is preferred over individual function resets.

[BZ#517460](#)<sup>1378</sup>

- When a migration was performed to a virtual machine that had been paused, the virtual machine would no longer be paused after the migration had completed. The behavior of **qemu-kvm** was changed so that it no longer 'forgets' the virtual machine is paused, and it will now stay paused during a migration.

[BZ#519204](#)<sup>1379</sup>

- **libvirt** was ordering disks unnecessarily. When a new disk was added, it would sometimes shift the boot disk later in the list, causing the user to be unable to boot. The sorting algorithm was changed, and will now insert a new disk as far to the end of the list as possible, while being ordered correctly with other disks on the same bus. This resolved booting errors caused by disk ordering.

[BZ#521053](#)<sup>1380</sup>

- A typographical error in an XML domain file caused **libvirtd** to suffer a segmentation fault. A check was added, and a typing mistake will now cause **libvirtd** to fail gracefully and produce a meaningful error report.

[BZ#523418](#)<sup>1381</sup>

- Devices that are assigned below a non-ACS switch can cause transactions to bypass the VT-d hardware and the validation process. **libvirt** now successfully blocks devices between non-ACS switches, unless the user specifies the `permissive='yes'` attribute for `<hostdev>`, so all transactions now undergo validation by default.

[BZ#526713](#)<sup>1382</sup>

- When querying Xen remotely `virsh` would sometimes raise an "unknown failure" error. The semantics were modified and where possible, the error is now more informative.

[BZ#531729](#)<sup>1383</sup>

- When using `xen+ssh://` to connect to a host, sometimes an RPC entry point would not be available and **dominfo** would raise an uninformative **error: unknown procedure** error. The error reporting was changed and it now reports as an unsupported entry point.

[BZ#531735](#)<sup>1384</sup>

- When a network created a bridge, it would only be enabled if the host had an IP on that bridge. This would cause the bridge creation to fail quietly, and packets would not be passed as expected. The error messages were improved for bridge creation and deletion, and if a failure occurs, it will now produce an informative error.

[BZ#532834](#)<sup>1385</sup>

- HVM VT-d PCI passthrough attach and detach was not working correctly and devices could not be hotplugged. The attach and detach code now has additional checks and hotplugging functions as expected.

[BZ#546671](#)<sup>1386</sup>

- When **virt-manager** tried to attach a PCI device to a Xen guest, it called **virNodeDeviceReset** and subsequently crashed. The Xen driver was updated, and it now checks if a given PCI device is assigned to another guest, so that PCI devices can be attached as expected.

[BZ#555309](#)<sup>1387</sup>

- When the host was running the KVM hypervisor, the **libvirtd** process was occasionally unable to connect to the hypervisor. In this case, **qemu-kvm** failed to start, and gave a false NUMA **out of**

**memory** error. The error handling was changed so that NUMA errors are now non-fatal. Errors are now logged, and connection progresses as expected.

[BZ#559755](#)<sup>1388</sup>

- **libvirt** was found to be incorrectly detecting machine types supported by KVM. This meant that KVM guests which did not specify any machine type could not be created. This also caused some rare problems that would cause `/distribution/virt/install` to fail. **libvirt** was updated to correctly detect and identify KVM-supported machine types.

[BZ#563151](#)<sup>1389</sup> & [BZ#569372](#)<sup>1390</sup>

These updated packages add the following enhancements:

- Support has been added for assigning Single Root I/O Virtualization (SR-IOV) devices to **qemu** guests.

[BZ#481748](#)<sup>1391</sup>

- Implementation of the **virsh dump** command for QEMU/KVM guests is included in this release.

[BZ#507551](#)<sup>1392</sup>

- Support was added to **libvirt** for KVM PCI device assignment hotplug.

[BZ#517465](#)<sup>1393</sup>

- Added **-mem-prealloc** to the KVM command line when using hugepage.

[BZ#518099](#)<sup>1394</sup>

- **libvirt** now allows the creation of more than 256 guests, and more than 150 DHCP leases.

[BZ#519729](#)<sup>1395</sup> & [BZ#524280](#)<sup>1396</sup>

- The **-M rhel5.4** arguments are now passed by default when launching **qemu-kvm**. This improves backward migration ability.

[BZ#542665](#)<sup>1397</sup>

Users of **libvirt** are advised to upgrade to these updated packages, which resolve these issues and add these enhancements.

## 1.108. libvirt-cim

### 1.108.1. RHBA-2009:1421: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1421](#)<sup>1398</sup>

An updated **libvirt-cim** package that fixes a bug is now available.

The libvirt-cim package is a Common Manageability Programming Interface (CMPI) CIM provider that implements the Distributed Management Task Force's (DMTF's) System Virtualization, Partitioning and Clustering (SVPC) virtualization model. This package supports most of the features of libvirt and enables management of multiple platforms with a single provider.

This updated libvirt-cim package fixes the following bug:

\* during installation, when the libvirt-cim package was selected in the KVM group, the xen package was installed as a dependency. This update removes the dependency on the xen package so that installing libvirt-cim does not cause the xen package to be installed. This is useful for customers who wish to use KVM virtualization with libvirt and libvirt-cim. ([BZ#517817](#)<sup>1399</sup>)

All users of libvirt-cim are advised to upgrade to this updated package, which resolves this issue.

### **1.108.2. RHBA-2010:0206: bug fix and enhancement update**

An updated libvirt-cim package which fixes a dependency error, adds support for domain console and network and storage pools in Red Hat Enterprise Linux 5.5 and re-bases the package from version 0.5.5 to version 0.5.8 is now available.

Libvirt-cim is a Common Manageability Programming Interface (CMPI) based Common Information Model (CIM) provider. It supports most libvirt virtualization features and allows for the management of multiple libvirt-based platforms.

This update addresses the following bug:

\* the libvirt-cim.spec file included a "Requires: xen" line. Consequently, selecting the libvirt-cim package in the KVM group during installation installed the xen package as a dependency. For this update, that line was removed and Xen is no longer installed automatically when libvirt-cim is installed. ([BZ#517579](#)<sup>1400</sup>)

Note: libvirt-cim is an optional package in the KVM group and will not be installed if only the KVM group is selected. The package has to be selected manually from the optional packages list to be installed.

Note: a workaround for this issue existed. It required not selecting libvirt-cim during installation and, after installation and registration of the system to the Red Hat Network (RHN), installing an updated libvirt-cim package from RHN. This workaround is no longer necessary.

This update also re-bases the package from version 0.5.5 to version 0.5.8. This re-base addresses several minor bugs as noted in the ChangeLog included in libvirt-cim.spec (available as part of the source rpm). The re-base also adds the following enhancement:

\* guest domain console support as well as support for storage pools and network pools was added. ([BZ#512233](#)<sup>1401</sup>)

All users of virtualization tools that interact with libvirt, especially those using CMPI and CIM, should install this updated package which addresses this problem and adds this enhancement.

---

<sup>1399</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=517817](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=517817)

<sup>1400</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=517579](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=517579)

<sup>1401</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=512233](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=512233)

## 1.109. libvorbis

### 1.109.1. RHSA-2009:1561: Important security update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2009:1561](#)<sup>1402</sup>

Updated libvorbis packages that fix multiple security issues are now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The libvorbis packages contain runtime libraries for use in programs that support Ogg Vorbis. Ogg Vorbis is a fully open, non-proprietary, patent-and royalty-free, general-purpose compressed audio format.

Multiple flaws were found in the libvorbis library. A specially-crafted Ogg Vorbis media format file (Ogg) could cause an application using libvorbis to crash or, possibly, execute arbitrary code when opened. ([CVE-2009-3379](#)<sup>1403</sup>)

Users of libvorbis should upgrade to these updated packages, which contain backported patches to correct these issues. The desktop must be restarted (log out, then log back in) for this update to take effect.

## 1.110. linuxwacom

### 1.110.1. RHEA-2010:0325: enhancement update

An enhanced linuxwacom package is now available.

The Linux Wacom Project manages the drivers, libraries, and documentation for configuring and running Wacom tablets under the Linux operating system. It contains diagnostic applications as well as X.org XInput drivers

\* support was added for the Intuos 4 tablet. ([BZ#566602](#)<sup>1404</sup>)

All users requiring Intuos 4 tablet support should install this new package, which adds this enhancement.

## 1.111. Im\_sensors

### 1.111.1. RHBA-2010:0186: bug fix and enhancement update

Updated Im\_sensors packages that fix a bug and add various enhancements are now available.

---

<sup>1403</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3379.html>

<sup>1404</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=566602](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=566602)

The `lm_sensors` package includes a collection of modules for general SMBus access and hardware monitoring.

These updated `lm_sensors` packages fix the following bug:

\* running the "sensors-detect" utility while redirecting input from `/dev/null` resulted in the following error message: "Use of uninitialized value in pattern match.../usr/sbin/sensors-detect". This spurious error message was caused by the referencing of an uninitialized variable, and has been fixed in this update. ([BZ#474383](https://bugzilla.redhat.com/show_bug.cgi?id=474383)<sup>1405</sup>)

In addition, these updated packages provide the following enhancements:

Important: the kernel update for Red Hat Enterprise Linux 5.5 includes updated `hwmon` kernel drivers that are necessary to enable newly-enabled sensor types. The Red Hat Enterprise Linux 5.5 kernel should therefore be installed along with this update.

\* `lm_sensors` now contains support for the `fschmd` driver, which means that the FSC Syleus chip is now supported. ([BZ#513099](https://bugzilla.redhat.com/show_bug.cgi?id=513099)<sup>1406</sup>)

\* the following devices are now supported ([BZ#473119](https://bugzilla.redhat.com/show_bug.cgi?id=473119)<sup>1407</sup>, [BZ#448223](https://bugzilla.redhat.com/show_bug.cgi?id=448223)<sup>1408</sup>, [BZ#443742](https://bugzilla.redhat.com/show_bug.cgi?id=443742)<sup>1409</sup>):

Analog Devices ADM1022, ADM1028 and ADM1029 Analog Devices ADT7470 Asus F71882FG and F71883FG FSC Heimdal Fintek F75373S/SG and F75375S/SP Fujitsu Technology Solutions Heracles, Hermes, Poseidon and Scylla Intel Core family thermal sensors Maxim MAX6650 and MAX6651 National Semiconductor LM93 and PC87427 SMSC DMF1737 SMSC SCH3112, SCH3114 and SCH3116 SMSC SCH5027D-NW and SCH5127 Texas Instruments THMC50 VIA VT1211 Winbond W83L786 NR/NG/R/G Winbond W83793 and R/G

Users of `lm_sensors` are advised to upgrade to these updated packages along with the Red Hat Enterprise Linux 5.5 kernel update. Doing so resolves this issue and add these enhancements.

## 1.112. log4cpp

### 1.112.1. RHEA-2010:0313: enhancement update

Updated `log4cpp` packages that add support for 32-bit x86 platforms are now available.

`log4cpp` is a library of C++ classes for flexible logging to files, syslog, IDSA and other destinations. It is modeled after the Log for Java library (<http://www.log4j.org>), staying as close to their API as is reasonable.

\* Only the 64-bit x86 version of `log4cpp` was provided previously. This updated package includes both 32-bit and 64-bit x86 platform versions of the library. ([BZ#552566](https://bugzilla.redhat.com/show_bug.cgi?id=552566)<sup>1410</sup>)

\* Installing both the 32-bit and 64-bit versions of the library in parallel caused a multilib conflict when the HTML documentation was built as part of the installation process. This prevented the installation of both versions on a single machine.

<sup>1405</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=474383](https://bugzilla.redhat.com/show_bug.cgi?id=474383)

<sup>1406</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=513099](https://bugzilla.redhat.com/show_bug.cgi?id=513099)

<sup>1407</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=473119](https://bugzilla.redhat.com/show_bug.cgi?id=473119)

<sup>1408</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=448223](https://bugzilla.redhat.com/show_bug.cgi?id=448223)

<sup>1409</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=443742](https://bugzilla.redhat.com/show_bug.cgi?id=443742)

<sup>1410</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=552566](https://bugzilla.redhat.com/show_bug.cgi?id=552566)



The HTML documentation was extracted to a separate package to allow multilib installation. ([BZ#502679](#)<sup>1411</sup>)

Users who wish to install both 32-bit and 64-bit versions for x86 platforms are advised to upgrade to these packages.

### 1.113. logwatch

#### 1.113.1. RHBA-2010:0033: bug fix and enhancement update



#### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2010:0033](#)<sup>1412</sup>

An updated logwatch package that fixes various bugs and adds an enhancement is now available.

LogWatch is a customizable log analysis system. LogWatch parses through your system's logs for a given period of time and creates a report analyzing areas that you specify, in as much detail as you require.

This updated logwatch package includes fixes for the following bugs:

\* .hdr files are headers for RPM packages; they are essentially metadata. LogWatch's HTTP service parser emitted warnings for .hdr files, even when the "Detail" parameter was set to "Low". With this update, .hdr files are now parsed as archives, which removes spurious warnings about .hdr files. ([BZ#465212](#)<sup>1413</sup>)

\* the following missing directories have been added under the /etc/logwatch/scripts/ directory: "logfile", "services" and "shared". This mirrors the subdirectory structure of the /usr/share/logwatch/scripts/ directory, and also corresponds to the existing documentation. ([BZ#489490](#)<sup>1414</sup>)

\* LogWatch attempted to interpret certain compressed log files as plain text log files, which resulted in binary information being written to LogWatch output. With this update, LogWatch correctly decompresses these compressed log files before attempting to read and interpret them. ([BZ#511928](#)<sup>1415</sup>)

In addition, this updated logwatch package provides the following enhancement: \* LogWatch is now able to parse several new and previously-unmatched entries in the postfix, dovecot and up2date application logs. ([BZ#460993](#)<sup>1416</sup>, [BZ#424031](#)<sup>1417</sup>, [BZ#466455](#)<sup>1418</sup>)

All users of logwatch are advised to upgrade to this updated package, which resolves these issues and provides this enhancement.

---

<sup>1411</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=502679](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=502679)

<sup>1413</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=465212](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=465212)

<sup>1414</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=489490](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=489490)

<sup>1415</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=511928](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=511928)

<sup>1416</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=460993](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=460993)

<sup>1417</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=424031](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=424031)

<sup>1418</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=466455](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=466455)

## 1.114. lvm2

### 1.114.1. RHBA-2009:1476: bug-fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1476](#)<sup>1419</sup>

Updated lvm2 packages that fix bugs are now available.

The lvm2 packages contain support for Logical Volume Management (LVM).

This update applies the following bug fixes:

\* Adds new option `prioritise_write_locks` in `lvm.conf`. Without enabling this option, whenever there are competing read-only and read-write access requests for a volume group's metadata, the write access may be stalled by a high volume of read-only requests.

NOTE: This option only affects `locking_type 1` (local file-based locking).

\* Make all tools use consistent lock ordering. This fixes `vgextend` command to block instead of failing when requested Volume Group is locked read-only.

\* Use read-only instead of write lock for `lvchange --refresh`.

\* Adds `global/wait_for_locks` to `lvm.conf` so blocking for locks can be disabled.

\* Fixes bug where non-blocking file locks could be granted in error.

All users of lvm2 are advised to upgrade to these updated packages, which resolve these issues.

### 1.114.2. RHBA-2009:1538: bug-fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1538](#)<sup>1420</sup>

Updated lvm2 packages that fix a bug are now available.

The lvm2 packages contain support for Logical Volume Management (LVM).

This update applies the following bug fix:

\* Fix default device mode permissions when using static lvm.

All users of lvm2 are advised to upgrade to these updated packages, which resolve this issue.

### 1.114.3. RHBA-2010:0298: bug fix and enhancement update

Updated lvm2 packages that fix several bugs and add enhancements are now available.

The lvm2 packages contain support for Logical Volume Management (LVM).

This update applies the following bug fixes:

- \* Fixes crash in dmevnetd if both snapshot and mirror monitoring is used.
- \* Fixes several memory locking problems which could lead to deadlocks.
- \* Uses read-only instead of write lock for lvchange --refresh.
- \* Fixes bug where non-blocking file locks could be granted in error.
- \* Uses fixed buffer to prevent stack overflow in persistent filter dump.
- \* Fixes default device mode permissions when using static lvm.
- \* Fixes return code of info call for query by uuid.
- \* Allows vgremove of a VG with PVs missing.
- \* Drops metadata cache after device was autorepaired and removed from VG.
- \* Removes missing flag in metadata if PV reappeared and is empty.
- \* Fixes unlocking of Volume Group in pvresize and toolib error paths.
- \* Removes log volume from metadata if initial deactivation fails.
- \* Fixes several memory leaks in pvs and pvdisplay commands.
- \* Dumps persistent device filter after every full scan.
- \* Refreshes device filters before full device rescan.
- \* Returns error status if vgchange fails to activate some volume.
- \* Restricts vgchange to activate only visible LVs.
- \* Fixes pvmove region\_size overflow for very large PVs.
- \* Fixes lvcreate and lvresize %PVS argument always to use sensible total size.
- \* Delays announcing mirror monitoring to syslog until initialisation succeeded.
- \* Doesn't attempt to deactivate an LV if any of its snapshots are in use.
- \* Fixes pvcreate string termination in duplicate uuid warning message.
- \* Makes lvchange --refresh only take a read lock on volume group.
- \* Makes lvconvert honour log mirror options combined with downconversion.
- \* Makes all tools use consistent lock ordering obtaining VG\_ORPHAN lock second.
- \* Fixes memory leak in vgsplit when re-reading the vg.
- \* Fixes crash in vg\_release.
- \* Explicitly requests fallback to default major number in device mapper.
- \* Rounds up requested readahead to at least one page and print warning.

\* Fixes mirror convert polling to ignore LV with different UUID.

As well, this update adds the following enhancements:

\* Uses `lvconvert --repair` instead of `vgreduce` in mirror `dmeventd` and introduces to use mirror image and log policies. In the event of a failure, the policy specified in `lvm.conf` will be used to determine what happens (for exact description see using `mirror_log_fault_policy` and `mirror_image_fault_policy` comments in `lvm.conf`).

\* Updates man pages, including `lvcreate`, `lvconvert` to explain `PhysicalVolume` parameter, document `--all` option, clarify use of PE ranges, mention `--repair` in `lvconvert` and document size units uniformly.

\* Adds new option `prioritise_write_locks` in `lvm.conf`. This option only affects `locking_type 1` (local file-based locking).

\* Introduces new read-only locking as `locking type 4`.

\* Adds `wait_for_locks` option to `lvm.conf` so blocking for locks can be disabled.

\* Adds an API version number, `LVM_LIBAPI`, to the `VERSION` string for `liblvm`.

\* Handles metadata with unknown segment types more gracefully.

\* Adds `--pvmetadatacopies` for `pvcreate`, `vgcreate`, `vgextend`, `vgconvert`.

\* Adds implicit `pvcreate` support to `vgcreate` and `vgextend`.

\* Recognises DRBD devices and handle them like MD mirror devices.

\* Checks MD devices for a partition table during device scan.

\* Adds extended device (`blkext`) and md partition (`mdp`) types to filters.

\* Distinguishes between powers of 1000 and powers of 1024 in unit suffixes (`si_unit_consistency` `lvm.conf` option).

\* Introduces automatic `data_alignment` detection and adds `devices/data_alignment_detection` to `lvm.conf`.

\* Adds `--dataalignmentoffset` to `pvcreate` to shift start of aligned data area.

\* Updates `'md_chunk_alignment'` to use `stripe-width` to align PV data area.

Users of `lvm2` are advised to upgrade to these updated packages, which resolve these issues and add these enhancements.

## 1.115. lvm2-cluster

### 1.115.1. RHBA-2009:1475: bug-fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1475<sup>1421</sup>](#)

Updated lvm2-cluster packages that fix several bugs are now available.

The lvm2-cluster packages contain support for Logical Volume Management (LVM) in a clustered environment.

This update applies the following bug fixes:

- \* Make all tools use consistent lock ordering. This fixes vgextend command to block instead of failing when requested Volume Group is locked read-only.
- \* Use read-only instead of write lock for lvchange --refresh.
- \* Adds global/wait\_for\_locks to lvm.conf so blocking for locks can be disabled.
- \* Fixes bug where non-blocking file locks could be granted in error.

Users of lvm2-cluster are advised to upgrade to these updated packages, which resolve these issues.

### **1.115.2. RHBA-2010:0299: bug fix and enhancement update**

Updated lvm2-cluster packages that fix several bugs and add enhancements are now available.

The lvm2-cluster packages contain support for Logical Volume Management (LVM) in a clustered environment.

This update ensures that the bugs fixed by the lvm2 advisory are also fixed in a clustered environment.

This update applies the following bug fixes:

- \* Fixes pvmove abort to be cluster-aware when temporary mirror activation fails.
- \* Always query active device by using uuid only in cluster.
- \* Unlocks shared lock in clvmd if device activation call failed.
- \* Fixes clvmd to never scan suspended devices.
- \* Never uses distributed lock for LV in non-clustered VG.
- \* Fixes clvmd memory leak in lv\_info\_by\_lvid.
- \* Fixes clvmd segfault when refresh\_toolcontext fails.
- \* Makes clvmd return 0 on success rather than 1.

This update adds the following enhancements:

- \* Propagates commit and revert metadata notifications to other nodes in cluster.
- \* Allows implicit convert to the same cluster lock mode.
- \* Adds LSB standard headers and functions to clvmd initscript.

Users of lvm2-cluster are advised to upgrade to these updated packages, which resolve these issues and add these enhancements.

## 1.116. man-pages

### 1.116.1. RHBA-2009:1574: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2009:1574](#)<sup>1422</sup>

An updated man-pages package that corrects numerous documentation errors and omissions is now available for Red Hat Enterprise Linux 5.

The man-pages package provides man (manual) pages from the Linux Documentation Project.

This updated man-pages package addresses the following issues:

- \* some shells (including bash, the default Red Hat Enterprise Linux shell) have a built-in "time" command. The time man page, however, documents `/usr/bin/time`, which provides options not available using the shell keyword equivalent. Previously, the time man page did not note this distinction. The time manual's DESCRIPTION section now notes both the existence of built-in time commands and that the man page documents `/usr/bin/time` and not these built-in shell keywords. ([BZ#443059](#)<sup>1423</sup>)
- \* the proc pseudo file system includes a series of process status information directories at `/proc/[number]/stat` (where [number] is the Process ID or PID). There are 42 status parameters but the proc man page did not document the 42nd, `delayacct_blkio_ticks`. This parameter, which returns aggregated block I/O delays, is now documented. ([BZ#452290](#)<sup>1424</sup>)
- \* the proc man page referenced two external files incorrectly. In the Description section, Memory Type Range Registers (`/proc/mtrr`) details were referenced to `/usr/src/linux/Documentation/mtrr.txt`. The See Also section, referenced `proc.txt` to `/usr/src/linux/Documentation/filesystems/`. The referenced files are in `/usr/share/doc/kernel-doc-2.6.18/Documentation/` and the proc man page now reflects this. ([BZ#456219](#)<sup>1425</sup>)
- \* the POSIX man pages -- in `/usr/share/man/man0p/`, `/usr/share/man/man1p/` and `/usr/share/man/man3p/` -- document applications that are not necessarily included with Red Hat Enterprise Linux but the documentation did not note this. These pages now have a boilerplate PROLOG section added that notes this explicitly. ([BZ#468897](#)<sup>1426</sup>)
- \* the syslog facility, LOG\_KERN, specified the kernel as the message source but did not note that this facility can be generated only by the kernel. The syslog man page now notes the LOG\_KERN facility cannot be generated from user processes. ([BZ#471176](#)<sup>1427</sup>)
- \* the `pthread_setaffinity_np` (part of `pthread.h`) man page was not included in the man-pages package. It now is. ([BZ#474238](#)<sup>1428</sup>)

<sup>1423</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=443059](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=443059)

<sup>1424</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=452290](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=452290)

<sup>1425</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=456219](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=456219)

<sup>1426</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=468897](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=468897)

<sup>1427</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=471176](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=471176)

<sup>1428</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=474238](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=474238)

\* the `/proc/sys/fs/file-nr` description in the `proc` man page still reflected `file-nr`'s use by version 2.4.x of the Linux kernel. This description has been updated to reflect the file's use in version 2.6 of the kernel. ([BZ#497197](#)<sup>1429</sup>)

\* the `gai.conf` man page included a repeated mis-spelling in its `EXAMPLE` section: `precedence`. This has been corrected to "precedence". ([BZ#515346](#)<sup>1430</sup>)

\* `zdump`, a tool which returns the time in each timezone listed on the command line, includes a "--version" switch which returns `zdump`'s version. The `zdump` man page did not list this option. The switch is now listed in the `SYNOPSIS` section as expected. ([BZ#517309](#)<sup>1431</sup>)

\* the `statfs` man page has been completely updated. As well, "man `statfs64`" now displays the `statfs` documentation rather than the `statfs64` page, which has been removed. This latter change removes a significant error in the previous (and prototype) `statfs64` `SYNOPSIS` section. ([BZ#518984](#)<sup>1432</sup>)

\* the `aliases` description in the `nsswitch.conf` man page was easily misconstrued to suggest aliases were not used at all. A re-written description makes it clear this database is used and clarifies the default `SendMail` configuration on Linux (which, by default, uses an alias resolution system independent of `/etc/nsswitch.conf`). ([BZ#522761](#)<sup>1433</sup>)

\* the `SOCKET OPTIONS` section of the `ip` man page listed `IP_MULTICAST_IF` as taking `ip_mreqn` or `ip_addr` arguments. This is incorrect: `IP_MULTICAST_IF` takes arguments with `ip_mreqn` or `in_addr` structures. This update corrects the error. ([BZ#524246](#)<sup>1434</sup>)

\* `/proc/sys/fs/file-max` defines a system-wide limit on the number of open files for all processes. This limit does not, however, apply to a root user (or any user with `CAP_SYS_ADMIN` privileges). This latter fact was not documented in the `proc` man page: it now is. ([BZ#527196](#)<sup>1435</sup>)

All man page users should upgrade to this updated package, which resolves these issues.

## 1.117. man-pages-ja

### 1.117.1. RHBA-2009:1630: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as `FASTRACK` errata [RHBA-2009:1630](#)<sup>1436</sup>

An updated `man-pages-ja` package that fixes documentation errors and typos is now available.

The `man-pages-ja` package contains Japanese translations of the Linux Documentation Project man pages.

---

<sup>1429</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=497197](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=497197)

<sup>1430</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=515346](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=515346)

<sup>1431</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=517309](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=517309)

<sup>1432</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=518984](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=518984)

<sup>1433</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=522761](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=522761)

<sup>1434</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=524246](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=524246)

<sup>1435</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=527196](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=527196)

This updated package corrects errors and fixes typos as follows:

\* the mkfs man page stated a file system could be built on a device (eg /dev/hda1) or the mount point for the file system (eg /usr or /home). The latter statement is incorrect: a file system can not be built on a file system's mount point. The English language version of the mkfs man page was corrected previously. With this update, the Japanese version has also been corrected. ([BZ#486655](https://bugzilla.redhat.com/show_bug.cgi?id=486655)<sup>1437</sup>)

\* the Japanese version of the less man page noted the application can identify Japanese character encodings from the LANG environment variable. This is not correct: with older versions of less, when LANG was set to Shift JIS (ja\_JP.SJIS) and less was run on a file that contains SJIS multi-byte characters, a "may be a binary file. See it anyway?" message was returned. To run less on files containing SJIS multi-byte characters, in addition to setting the appropriate LANG environment variable, the LESSCHARSET environment variable had to be set to "dos". This update removes documentation related to Japanese-specific features of older version of less (including the details noted above). ([BZ#509048](https://bugzilla.redhat.com/show_bug.cgi?id=509048)<sup>1438</sup>)

\* the strings command takes a "--byte=min-len" option but the Japanese strings man page presented this option as "-byte=min-len" (ie, with a missing initial hyphen). This error has been corrected. Note: attempting to run strings with, in effect, a "-b" option returns an "invalid option -- b" error, along with help text noting the "--bytes=[number]" option. ([BZ#515467](https://bugzilla.redhat.com/show_bug.cgi?id=515467)<sup>1439</sup>)

\* the chgrp command's "--dereference" option is the default, and is documented as such in the English language chgrp man page. Previously, however, the Japanese translation erroneously listed "-h" or "--no-dereference" as the default. This error has been corrected and the Japanese chgrp man page now correctly lists "--dereference" as the default option. [BZ#527638](https://bugzilla.redhat.com/show_bug.cgi?id=527638)<sup>1440</sup>

\* the SOCKET OPTIONS section of the ip man page listed IP\_MULTICAST\_IF as taking ip\_mreqn or ip\_addr arguments. This is incorrect: IP\_MULTICAST\_IF takes arguments with ip\_mreqn or in\_addr structures. This update corrects the error. Note: the same error was present in the original English man page. The English-language error was corrected in Red Hat Enterprise Linux 5 via the man pages bug fix update, RHBA-2009-1574. ([BZ#537103](https://bugzilla.redhat.com/show_bug.cgi?id=537103)<sup>1441</sup>)

\* the previous release of man-pages-ja contained an older version of the hostname man page which did not document all available command options. This has been corrected: this new man-pages-ja release includes an up-to-date man page which documents all of the hostname command's options. ([BZ#533782](https://bugzilla.redhat.com/show_bug.cgi?id=533782)<sup>1442</sup>)

\* the elvtune command is deprecated for Linux kernel version 2.6 and it is not shipped with Red Hat Enterprise Linux 5. the elvtune man page was still included in the man-pages-ja package, however. With this update, the elvtune man page has been removed to avoid confusion. ([BZ#519707](https://bugzilla.redhat.com/show_bug.cgi?id=519707)<sup>1443</sup>)

All man-pages-ja users should upgrade to this updated package, which resolves these issues.

---

<sup>1437</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=486655](https://bugzilla.redhat.com/show_bug.cgi?id=486655)

<sup>1438</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=509048](https://bugzilla.redhat.com/show_bug.cgi?id=509048)

<sup>1439</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=515467](https://bugzilla.redhat.com/show_bug.cgi?id=515467)

<sup>1440</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=527638](https://bugzilla.redhat.com/show_bug.cgi?id=527638)

<sup>1441</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=537103](https://bugzilla.redhat.com/show_bug.cgi?id=537103)

<sup>1442</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=533782](https://bugzilla.redhat.com/show_bug.cgi?id=533782)

<sup>1443</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=519707](https://bugzilla.redhat.com/show_bug.cgi?id=519707)



### 1.118. mcelog

#### 1.118.1. RHBA-2010:0247: bug fix update

An updated mcelog package that restricts mcelog operation on para-virtualized guests running under the Xen hypervisor is now available.

mcelog is a daemon that collects and decodes Machine Check Exception data on AMD64- and Intel 64-based systems.

This update addresses the following issue:

\* in some circumstances, mcelog can run on para-virtualized guest operating systems (domU) running under the Xen hypervisor (dom0). This results in near 100% cpu usage on the guest, with the mcelog process blocking all other processes. This update adds a check to `/etc/cron.hourly/mcelog.cron`: if the check finds it is running on a para-virtualized guest, it exits, ensuring mcelog does not execute in such circumstances. ([BZ#522827](#)<sup>1444</sup>)

All mcelog users should install this this new mcelog package, which adds the check to resolve this issue.

### 1.119. mdadm

#### 1.119.1. RHBA-2010:0006: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2010:0006](#)<sup>1445</sup>

An updated mdadm package that fixes a bug is now available.

mdadm is used to create, manage, and monitor Linux MD (software RAID) devices. It provides similar functionality to the raidtools package.

This updated package fixes the following bug:

\* the previous mdadm update added a data scrubbing cron job, `/etc/cron.weekly/99-raid-check`, that looks for bad sectors on drives in redundant arrays and fixes the bad sectors using data from other drives to reconstruct sectors that return read errors. The script only performs checks on idle, healthy arrays but, previously, it initiated each check operation in turn, and switched idle arrays to active as it went. Consequently, if different arrays shared the same physical drive, the `raid-check` script only checked one of the arrays on that drive. With this update the `raid-check` script now gets the the state from all arrays on all drives before initiating the first check operation. Multiple arrays on a single device are now checked by the `raid-check` script as expected. ([BZ#523000](#)<sup>1446</sup>)

All mdadm users are advised to upgrade to this updated package, which resolves these issues and adds this feature.

---

<sup>1444</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=522827](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=522827)

<sup>1446</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=523000](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=523000)

## 1.120. mesa

### 1.120.1. RHBA-2010:0261: bug fix update

Updated mesa packages that fix a bug in xorg-x11-server are now available.

Mesa provides a 3D graphics API that is compatible with OpenGL. It also provides hardware-accelerated drivers for many popular graphics chips.

This update addresses the following issue:

\* the OpenGL Extension to the X Window system (GLX) provides OpenGL functions to X Windows-based applications. Previously, when a so-called 'GLX window' (ie a window drawn by an X Windows-based application containing OpenGL rendered data) was re-sized horizontally on a system with Mobile Intel 945GM Express video hardware, the X session segfaulted. As well, re-sizing such a window vertically and then maximizing and restoring the window also caused X to segfault. This updated mesa package includes a fix to the frambuffer code that properly signals the changed buffer state to the driver, ensuring the driver updates its clipping and does not, as a consequence, cause X to crash. ([BZ#536868](#)<sup>1447</sup>)

Note: due to the unusual build process for this package, the code fix is applied to the mesa packages, but the resulting compiled code is in the xorg-x11-server package (see [BZ#435963](#)<sup>1448</sup> for the bug as raised against xorg-x11-server).

All users compiling their own xorg-x11-server packages should upgrade to these updated mesa packages, which resolves this issue.

## 1.121. metacity

### 1.121.1. RHBA-2009:1610: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1610](#)<sup>1449</sup>.

An updated metacity package that fixes a raising windows bug and corrects a crash with remotely displayed applications is now available.

Metacity is the default window manager for the GNOME desktop.

This errata fixes two bugs in the metacity package:

\* some applications, mostly older Tcl/Tk and Java applications, use the old XRaiseWindow call rather than `_NET_ACTIVE_WINDOW` to raise a window above the currently focused window. Metacity allows XRaiseWindow when the same application keeps focus but defines an application by its window group. Some of these older applications also do not set the window group and, consequently, metacity

<sup>1447</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=536868](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=536868)

<sup>1448</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=435963](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=435963)

did not honor window-raising requests from such applications. With this update, metacity expands its checking to allow the same X client (defined as having the same client ID) to raise windows above the currently focused window using the old XRaiseWindow call. Older Tcl/Tk and Java applications, in particular, should now behave as expected. ([BZ#537023](https://bugzilla.redhat.com/show_bug.cgi?id=537023)<sup>1450</sup>)

\* Incorrectly placed error traps meant, when an application window running on a remote computer with its display forwarded to the local system was closed, metacity sometimes crashed with an "Unexpected X error: BadWindow (invalid Window parameter)" error. The error trap has been moved in this update and closing forwarded windows now closes the remote application as expected. ([BZ#537024](https://bugzilla.redhat.com/show_bug.cgi?id=537024)<sup>1451</sup>)

Users are advised to upgrade to this updated metacity package which resolves these issues.

### 1.121.2. RHBA-2010:0245: bug fix and enhancement update

An updated metacity package that fixes numerous bugs and adds several enhancements is now available

Metacity is the default window manager for the GNOME desktop.

This update fixes the following bugs:

\* if a modal dialog box was open, its associated window could not be moved to another workspace. The dialog box would stay on the current desktop but the main window would vanish as it moved and then returned but no longer displayed correctly. The `meta_workspace_focus_default_window()` has been modified so that windows can now be dragged to other workspaces even if a modal dialog box is open. ([BZ#237158](https://bugzilla.redhat.com/show_bug.cgi?id=237158)<sup>1452</sup>)

\* dragging a maximized window between monitors on a system configured to use a Xinerama dual-screen configuration caused flickering. Metacity has been modified to allow one to move maximized windows meaning they can be dragged between monitors without flickering. ([BZ#495939](https://bugzilla.redhat.com/show_bug.cgi?id=495939)<sup>1453</sup>)

\* Metacity was preventing applications such as Maya from stacking windows correctly. This was caused by the focus-stealing prevention mechanism. A patch has been added to allow stacking to occur, meaning module windows for tools like Maya now work in the expected fashion. ([BZ#503522](https://bugzilla.redhat.com/show_bug.cgi?id=503522)<sup>1454</sup>)

\* the `/apps/metacity/general/strict_focus_mode` option can be activated via GConf to prevent focus from being stolen from a terminal window. On x86\_64 systems, terminals were sometimes not recognized as this function was incorrectly implemented: it was looking for `res_name` instead of `res_class`. Metacity now checks the `res_class` to determine if a window is a terminal and focus is no longer lost. ([BZ#504223](https://bugzilla.redhat.com/show_bug.cgi?id=504223)<sup>1455</sup>)

\* if the user switched between workspaces, any open KDE applications would start to flash in GNOME as Metacity mistakenly marked them as needing user intervention. Metacity now checks the window to determine if it has a "startup ID" and sets the `initial_timestamp` and `initial_workspace` properties accordingly. As a result KDE applications no longer flash in these circumstances. ([BZ#506537](https://bugzilla.redhat.com/show_bug.cgi?id=506537)<sup>1456</sup>)

---

<sup>1450</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=537023](https://bugzilla.redhat.com/show_bug.cgi?id=537023)

<sup>1451</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=537024](https://bugzilla.redhat.com/show_bug.cgi?id=537024)

<sup>1452</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=237158](https://bugzilla.redhat.com/show_bug.cgi?id=237158)

<sup>1453</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=495939](https://bugzilla.redhat.com/show_bug.cgi?id=495939)

<sup>1454</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=503522](https://bugzilla.redhat.com/show_bug.cgi?id=503522)

<sup>1455</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=504223](https://bugzilla.redhat.com/show_bug.cgi?id=504223)

<sup>1456</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=506537](https://bugzilla.redhat.com/show_bug.cgi?id=506537)

\* Metacity could not handle closing application windows run remotely via X. A BadWindow error would occur. A patch has been added to trap this error. As a result, the error message no longer appears. ([BZ#523777](https://bugzilla.redhat.com/show_bug.cgi?id=523777)<sup>1457</sup>)

\* when the `/apps/metacity/general/raise_on_click` GConf key was set to "false" this option incorrectly combined the ability to intercept user clicks with the intended use of intercepting calls coming from applications. Consequently, windows for many non-EWMH (Extended Window Manager Hints) compliant applications could not be raised or lowered. This issue has now been rectified so that, if the key is set to false, older applications not yet using `net_window_activate` can be raised and lowered. ([BZ#526045](https://bugzilla.redhat.com/show_bug.cgi?id=526045)<sup>1458</sup>)

This update also adds the following enhancements:

\* in Metacity's "mouse" and "sloppy" focus modes, it is possible to have the pointer hover over a window without it becoming focused. This happens, for example, if another window steals focus away. Previously, it was necessary to move the mouse out of the window and then back into it, or to click on it, to give it focus. ([BZ#530261](https://bugzilla.redhat.com/show_bug.cgi?id=530261)<sup>1459</sup>)

\* the `/apps/metacity/general/place_on_current_monitor` feature was added. If this option is set to "true", new windows will always be placed on the current monitor, rather than be placed on any monitor with free space. ([BZ#523841](https://bugzilla.redhat.com/show_bug.cgi?id=523841)<sup>1460</sup>)

\* if an application displays a window without setting its appropriate properties, it steals focus from the current window and thereby steal the user's keystrokes. (This usually happens with older applications written without modern toolkits.) The new `no_focus_windows` option allows one to specify which windows should not be given the keyboard's focus. ([BZ#530262](https://bugzilla.redhat.com/show_bug.cgi?id=530262)<sup>1461</sup>)

\* when a new window is not given keyboard focus, it is placed underneath the current window and entry flashes. When the new `/apps/metacity/general/new_windows_always_on_top` key is set to "true", windows are always placed on top, irrespective of keyboard focus. ([BZ#530263](https://bugzilla.redhat.com/show_bug.cgi?id=530263)<sup>1462</sup>)

Users are advised to upgrade to this updated Metacity package, which resolve these issues and adds these enhancements.

## 1.122. microcode\_ctl

### 1.122.1. RHEA-2010:0243: enhancement update

An updated `microcode_ctl` package that provides the latest version of the Intel microcode is now available.

`microcode_ctl` provides utility code and the microcode data itself -- supplied by Intel -- to assist the kernel in updating the CPU microcode at system boot time. This microcode supports all current Intel x86- and Intel 64-based CPU models and takes advantage of the mechanism built-in to Linux that allows microcode to be updated after system boot. When loaded, the updated microcode corrects the behavior of various Intel processors, as described in processor specification updates issued by Intel for those processors.

<sup>1457</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=523777](https://bugzilla.redhat.com/show_bug.cgi?id=523777)

<sup>1458</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=526045](https://bugzilla.redhat.com/show_bug.cgi?id=526045)

<sup>1459</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=530261](https://bugzilla.redhat.com/show_bug.cgi?id=530261)

<sup>1460</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=523841](https://bugzilla.redhat.com/show_bug.cgi?id=523841)

<sup>1461</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=530262](https://bugzilla.redhat.com/show_bug.cgi?id=530262)

<sup>1462</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=530263](https://bugzilla.redhat.com/show_bug.cgi?id=530263)

This update provides the following enhancement:

\* this package contains the 2009-09-27 update to Intel's microcode. As of 2010-01-22, this is the most recent version of the microcode available from Intel. ([BZ#526802](#)<sup>1463</sup>)

All users running systems based on Intel processors are encouraged to install this update, which adds the most up-to-date microcode data from Intel to `/etc/firmware` as required. Note: a system reboot is necessary for the this update to take effect.

## 1.123. mkinitrd

### 1.123.1. RHBA-2010:0295: bug fix and enhancement update

The `mkinitrd` utility creates file system images for use as initial ramdisk (initrd) images.

These updated packages address the following bugs:

- booting a Storage Area Network (SAN) from a replicated Logical Unit Number (LUN) following a loss of the primary site would fail when doing array-based synchronous data replication to a remote site. This was due to the fact that the `initrd` on the replicated LUN is configured to see the World Wide Identifier (WWID) of the primary LUN only. A patch has been applied that allows for the creation of all multipath devices so that the replicated LUN is visible for booting. It should be noted that some manual configuration is required following the installation of the updated package:

1. ensure that `multipath.conf` has the correct stanzas for *both* multipath devices.
2. run `mkinitrd` again.

A replicated LUN will now successfully boot provided:

- a. the `multipath.conf` in the `initrd` does not blacklist the new LUN and;
- b. `/var/lib/multipath/bindings` in the `initrd` is either empty or contains an entry binding `mpath0` (or the device originally installed to) to the replicated LUN's WWID.

([BZ#438887](#)<sup>1464</sup>)

- `scsi_model devflag` options appended to `/etc/modprobe.conf` can be of the form: "options `scsi_mod dev_flags="HITACHI:OPEN-9 -SUN:0x240"` to specify more than one SCSI model. These strings are written as arguments to the `insmod` command within the `initrd` script. The leading spaces of the second model name in the above example were incorrectly read as a single space by the `nash` command resulting in the `/proc/scsi/device_info` file containing invalid strings. A user specifying a SCSI model in this way would have to manually edit the `/proc/scsi/device_info` file as a result. A patch has been applied to `nash.c` to correctly handle the quoted string following the `dev_flag` argument. The string is now written to the `/proc/scsi/device_info` file in the correct format. ([BZ#467850](#)<sup>1465</sup>)
- `mkinitrd` uses a global variable `rootdev` to store the name of the root device. This is either auto-detected or passed in via the command line `--rootdev=` parameter. Changes applied to `mkinitrd` to support **boot from multipath** introduced the local `rootdev` variable. This variable overrides the global variable resulting in an incorrect root device, such as a component

---

<sup>1463</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=526802](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=526802)

SCSI device, being written to the `/init` script preventing the system from booting. The local variable has been renamed to avoid the conflict. Running `mkinitrd` on a multipath boot system now results in a successful boot of the system. ([BZ#503567](#)<sup>1466</sup>)

- `mkinitrd` runs `nash` on each logical volume. The `block_find_fs_by_key()` method calls the `nashDmGetDevName()` method for each logical volume. The `nash` command does not run to completion in a reasonable time-frame as the `nashDmGetDevName()` recurses through all devices each time it is called. This update allows `nashDmGetDevName()` to cache its results, so `nash` no longer uses 100% of the CPU when installing `RPMs`. ([BZ#516047](#)<sup>1467</sup>)
- `mkinitrd` copied the `lvm.conf` file verbatim to the `initrd` without parsing it properly. If the logical volume manager (LVM) was configured to use host tags, **Red Hat Enterprise Linux** would not boot because a host name could not be set at `initrd` time. `lvm --dumpconfig` is now used to retrieve the LVM configuration file. ([BZ#517868](#)<sup>1468</sup>)
- `mkinitrd` attempted to explicitly activate the subsets of a nested RAID 10 set. Error messages would then be printed to the log during boot. These messages could safely be ignored. They have now been removed to avoid confusion. ([BZ#526246](#)<sup>1469</sup>)
- `mkinitrd` copied the symbolic link of a bootpath driver instead of the actual bootpath driver. This caused kernel panic due to an unavailable driver on first boot of the operating system. `mkinitrd` now checks the full path of symbolically linked drivers. ([BZ#540641](#)<sup>1470</sup>)
- when the root file system was on the logical volume manager (LVM), as is the default installation option, `nash` received a segmentation fault reference if some modules did not load during post-installation reboot. This caused unwarranted kernel panic. Kernel panic no longer occurs as a result of the non-loading of modules. ([BZ#560567](#)<sup>1471</sup>)
- several `virtio` modules were missing from the previous version of `mkinitrd`. This meant that `mkinitrd` built incorrectly upon installation if `virtio` block or network devices were used within the **Kernel Based Virtual Machine** (KVM). The final result was kernel panic. These updated packages contain the required modules which allow `mkinitrd` to build and install correctly. ([BZ#560672](#)<sup>1472</sup>)

As well, these updated packages add the following enhancements:

- the `scsi_dh_rdac` module is needed to support many LSI Engenio based (IBM and non-IBM) storage devices. With the inclusion of a module such as the `scsi_dh_rdac` module in `initrd`, the time to boot a system with multiple `rdac` devices is minimized. A patch has been applied to `mkinitrd` to load every `scsi_dh_*` module in the event that multipath devices are detected. The patch currently succeeds in loading `xscsi_dh_rdac` modules for installations on DS4K storage and further work is being undertaken to ensure the successful loading of modules independent of the host device. ([BZ#460899](#)<sup>1473</sup>)
- `mkinitrd` is responsible for ensuring that all drivers, applications, and configuration information needed to mount the root filesystem are packaged into each kernel's `initrd`. Unlike the Logical Volume Manager (LVM) component of `mkinitrd`, multipath operates on only the *logical volume* associated with the root filesystem and not the *volume group* containing the root filesystem. As a consequence, when installing a system with multipath devices, only disks currently in use by the root's logical volume have multipath configured within the `initrd`. A patch has been applied that wraps the `find_mpath_deps` in a loop that iterates through every primary volume in the root volume group. Non-LVMs are handled in a separate case by running `find_mpath_deps` against the root device. Installing a system with multipath devices will now result in the primary volumes in the root virtual group being on multipath devices. ([BZ#501535](#)<sup>1474</sup>)

Users of `mkinitrd` are advised to upgrade to these updated packages, which resolve these issues and add these enhancements.

### 1.124. module-init-tools

#### 1.124.1. RHBA-2010:0242: bug fix update

Update `module-init-tools` packages that fix several bugs are now available.

The `module-init-tools` package includes various programs needed for automatic loading and unloading of modules under 2.6 and later kernels, as well as other module management programs. Device drivers and filesystems are two examples of loaded and unloaded modules.

The updated packages fix the following bugs:

\* on Xen systems with more than one detected serial device, a race condition could occur between simultaneously executed `modprobe` module loading utility commands if the Xen Hypervisor was blocking access or was misconfigured. The updated packages implement a read-only filesystem locking mechanism that prevents `modprobe` race conditions from occurring. ([BZ#430942](#)<sup>1475</sup>)

\* on systems where a driver update was removed and no compatible driver update exists after the removal, the `weak-module` post-installation scripts created symbolic links to the location of the deleted driver. This caused problems with driver updates, and using the `weak-module` utility. The updated packages ensure post-installation scripts create valid symbolic links to installed drivers. ([BZ#477089](#)<sup>1476</sup>)

\* on systems running Xen hypervisor compatible kernels, where the kernel is used as a guest kernel (Dom0) and not as a host kernel (DomU), the scripts that perform module post-install checks could regenerate an incorrect bootloader entry for the system. In some cases, this prevented the system from booting. The updated packages implement revised post-install checks, which prevent this scenario from occurring. ([BZ#509568](#)<sup>1477</sup>)

All `module-init-tools` users are advised to upgrade to these updated packages, which resolve these issues.

### 1.125. mtx

#### 1.125.1. RHBA-2009:1607: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2009:1607](#)<sup>1478</sup>

An updated `mtx` package that fixes one bug is now available.

---

<sup>1475</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=430942](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=430942)

<sup>1476</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=477089](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=477089)

<sup>1477</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=509568](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=509568)



The mtX package contains utilities that control single or multi-drive SCSI media changers such as tape changers, autoloaders, tape libraries, or optical media jukeboxes. It can also be used with media changers that use the 'ATTACHED' API, presuming that they properly report the MChanger bit as required by the SCSI T-10 SMC specification.

This updated package provides a fix for the following bug:

\* if the scsitape utility was run with an unknown command-line option (eg "-h", a switch option not used by scsitape), the application crashed with a Segmentation fault error. This update adds a termination entry to the end of the pertinent scsitape array. When an unknown command-line option is used, scsitape now exits cleanly and returns usage documentation to std out. ([BZ#513984](https://bugzilla.redhat.com/show_bug.cgi?id=513984)<sup>1479</sup>)

All mtX users should upgrade to this updated package, which resolves this issue.

## 1.126. mysql

### 1.126.1. RHBA-2009:1693: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1693](https://errata.redhat.com/errata/RHBA-2009:1693)<sup>1480</sup>

Updated mysql packages that fix a bug are now available.

MySQL is a multi-user, multi-threaded SQL database server. MySQL is a client/server implementation consisting of a server daemon (mysqld) and many different client programs and libraries.

These updated mysql packages fix a bug which occurred after updating the mysql packages from version 5.0.45, which was released as a part of Red Hat Enterprise Linux 5.2, to version 5.0.77, which was released as part of the Red Hat Enterprise Linux 5.4 update. A MySQL slave server could crash during replication if a DATE or DATETIME type was compared to the result of the NAME\_CONST() function, which commonly happens when stored procedures are used alongside replication. Also, following such a crash, the slave server would be restarted, perform crash recovery, and then crash again once it reached the same point where it performs the comparison, and repeat this cycle continuously. This has been fixed in these updated packages so that the slave server does not crash during replication if a DATE or DATETIME type is compared with the result of the NAME\_CONST() function. ([BZ#538731](https://bugzilla.redhat.com/show_bug.cgi?id=538731)<sup>1481</sup>)

All mysql users, and especially those using replication, are advised to upgrade to these updated packages, which resolve this issue.

<sup>1479</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=513984](https://bugzilla.redhat.com/show_bug.cgi?id=513984)

<sup>1481</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=538731](https://bugzilla.redhat.com/show_bug.cgi?id=538731)



### 1.126.2. RHSA-2010:0109: Moderate security update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2010:0109](#)<sup>1482</sup>

Updated mysql packages that fix multiple security issues are now available for Red Hat Enterprise Linux 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

MySQL is a multi-user, multi-threaded SQL database server. It consists of the MySQL server daemon (mysqld) and many client programs and libraries.

It was discovered that the MySQL client ignored certain SSL certificate verification errors when connecting to servers. A man-in-the-middle attacker could use this flaw to trick MySQL clients into connecting to a spoofed MySQL server. ([CVE-2009-4028](#)<sup>1483</sup>)

Note: This fix may uncover previously hidden SSL configuration issues, such as incorrect CA certificates being used by clients or expired server certificates. This update should be carefully tested in deployments where SSL connections are used.

A flaw was found in the way MySQL handled SELECT statements with subqueries in the WHERE clause, that assigned results to a user variable. A remote, authenticated attacker could use this flaw to crash the MySQL server daemon (mysqld). This issue only caused a temporary denial of service, as the MySQL daemon was automatically restarted after the crash. ([CVE-2009-4019](#)<sup>1484</sup>)

When the "datadir" option was configured with a relative path, MySQL did not properly check paths used as arguments for the DATA DIRECTORY and INDEX DIRECTORY directives. An authenticated attacker could use this flaw to bypass the restriction preventing the use of subdirectories of the MySQL data directory being used as DATA DIRECTORY and INDEX DIRECTORY paths. ([CVE-2009-4030](#)<sup>1485</sup>)

Note: Due to the security risks and previous security issues related to the use of the DATA DIRECTORY and INDEX DIRECTORY directives, users not depending on this feature should consider disabling it by adding "symbolic-links=0" to the "[mysqld]" section of the "my.cnf" configuration file. In this update, an example of such a configuration was added to the default "my.cnf" file.

All MySQL users are advised to upgrade to these updated packages, which contain backported patches to resolve these issues. After installing this update, the MySQL server daemon (mysqld) will be restarted automatically.

---

<sup>1483</sup> <https://www.redhat.com/security/data/cve/CVE-2009-4028.html>

<sup>1484</sup> <https://www.redhat.com/security/data/cve/CVE-2009-4019.html>

<sup>1485</sup> <https://www.redhat.com/security/data/cve/CVE-2009-4030.html>

## 1.127. nautilus-open-terminal

### 1.127.1. RHBA-2009:1483: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata *RHBA-2009:1483*<sup>1486</sup>

An updated nautilus-open-terminal package that fixes a bug is now available.

The nautilus-open-terminal extension provides a right-click "Open Terminal" option for Nautilus users who prefer that option.

This updated nautilus-open-terminal package fixes the following bug:

\* right-clicking on the GNOME desktop and selecting "Open Terminal" from the context menu always caused a new terminal window to open on the primary screen, even if "Open Terminal" was chosen on the second screen of a dual-monitor setup. With this update, newly-opened terminal windows correctly appear on the screen on which the "Open Terminal" unction is selected. (*BZ#509878*<sup>1487</sup>)

All users of nautilus-open-terminal are advised to upgrade to this updated package, which resolves this issue.

## 1.128. neon

### 1.128.1. RHSA-2009:1452: Moderate security update



#### Important

This update has already been released (prior to the GA of this release) as the security errata *RHSA-2009:1452*<sup>1488</sup>

Updated neon packages that fix two security issues are now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

neon is an HTTP and WebDAV client library, with a C interface. It provides a high-level interface to HTTP and WebDAV methods along with a low-level interface for HTTP request handling. neon supports persistent connections, proxy servers, basic, digest and Kerberos authentication, and has complete SSL support.

It was discovered that neon is affected by the previously published "null prefix attack", caused by incorrect handling of NULL characters in X.509 certificates. If an attacker is able to get a carefully-crafted certificate signed by a trusted Certificate Authority, the attacker could use the certificate during

<sup>1487</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=509878](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=509878)

a man-in-the-middle attack and potentially confuse an application using the neon library into accepting it by mistake. ([CVE-2009-2474](https://www.redhat.com/security/data/cve/CVE-2009-2474.html)<sup>1489</sup>)

A denial of service flaw was found in the neon Extensible Markup Language (XML) parser. A remote attacker (malicious DAV server) could provide a specially-crafted XML document that would cause excessive memory and CPU consumption if an application using the neon XML parser was tricked into processing it. ([CVE-2009-2473](https://www.redhat.com/security/data/cve/CVE-2009-2473.html)<sup>1490</sup>)

All neon users should upgrade to these updated packages, which contain backported patches to correct these issues. Applications using the neon HTTP and WebDAV client library, such as cadaver, must be restarted for this update to take effect.

## 1.129. net-snmp

### 1.129.1. RHBA-2009:1437: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1437](https://errata.redhat.com/errata/RHBA-2009:1437)<sup>1491</sup>

Updated net-snmp packages that resolve several issues are now available.

The Simple Network Management Protocol (SNMP) is a protocol used for network management. The net-snmp packages include various SNMP tools: an extensible agent, an SNMP library, tools for requesting or setting information from SNMP agents, tools for generating and handling SNMP traps, a version of the netstat command which uses SNMP, and a Tk/Perl MIB browser.

These updated net-snmp packages provide fixes for the following bugs:

\* snmpd, the SNMP daemon, did not expect the packet counters in the `/proc/net/snmp` and `/proc/net/snmp6` directories to be 64-bit on 64-bit systems. When these counters exceeded 32 bits in size, which would occur when the Linux kernel sent or received greater than 4,294,967,296 ( $2^{32}$ ) packets, then the snmpd daemon would terminate abnormally. With this update, the snmpd daemon no longer crashes when it encounters a packet counter in the directories listed above that is greater than 32 bits in size, thus resolving the issue. ([BZ#516183](https://bugzilla.redhat.com/show_bug.cgi?id=516183)<sup>1492</sup>)

\* snmpd, the SNMP daemon, contained several memory leaks in the `ipNetToMediaTable` module. These leaks caused snmpd to leak memory relatively slowly, but at a rate which could cause problems on machines with multi-month uptimes. These memory leaks have been plugged in these updated packages so that snmpd no longer leaks memory slowly. ([BZ#517041](https://bugzilla.redhat.com/show_bug.cgi?id=517041)<sup>1493</sup>)

All users of net-snmp are advised to upgrade to these updated packages, which resolve these issues.

### 1.129.2. RHBA-2010:0253: bug fix and enhancement update

Updated net-snmp packages that fix various bugs and add enhancements are now available.

---

<sup>1489</sup> <https://www.redhat.com/security/data/cve/CVE-2009-2474.html>

<sup>1490</sup> <https://www.redhat.com/security/data/cve/CVE-2009-2473.html>

<sup>1492</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=516183](https://bugzilla.redhat.com/show_bug.cgi?id=516183)

<sup>1493</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=517041](https://bugzilla.redhat.com/show_bug.cgi?id=517041)

The Simple Network Management Protocol (SNMP) is a protocol used for network management. The net-snmp packages include various SNMP tools: an extensible agent; an SNMP library; tools for requesting or setting information from SNMP agents; tools for generating and handling SNMP traps; a version of the netstat command which uses SNMP; and a Tk/Perl MIB browser.

These updated net-snmp packages provide fixes for the following bugs:

\* when two default routes with the same content existed in the machine's routing table, the snmpd daemon could have entered an endless loop and logged the following error to syslog: "error on subcontainer 'dr\_index' insert(-1)". Processing of the routing table has been improved in this update so that snmpd no longer enters an endless route when this occurs. ([BZ#504742](https://bugzilla.redhat.com/show_bug.cgi?id=504742)<sup>1494</sup>)

\* on 64-bit systems experiencing very high network traffic, the snmpd daemon periodically logged the following message to syslog: "truncating integer value > 32 bits". With this update, snmpd correctly adjusts reported counters and no error is logged. ([BZ#507528](https://bugzilla.redhat.com/show_bug.cgi?id=507528)<sup>1495</sup>)

\* the snmpd daemon did not expect the packet counters in the /proc/net/snmp and /proc/net/snmp6 directories to be 64-bit on 64-bit systems. When these counters exceeded 32 bits in size, which occurred when the Linux kernel sent or received greater than 4,294,967,296 (2<sup>32</sup>) packets, then the snmpd daemon would terminate abnormally. With this update, the snmpd daemon no longer crashes when it encounters a packet counter in the directories listed above that is greater than 32 bits in size, thus resolving the issue. ([BZ#514703](https://bugzilla.redhat.com/show_bug.cgi?id=514703)<sup>1496</sup>)

\* the snmpd daemon contained several memory leaks in the ipNetToMediaTable, mteEventSetTable and ipAddressPrefixTable objects. These slow memory leaks could have caused problems on machines with multi-month uptimes. These memory leaks have been plugged in these updated packages. ([BZ#518633](https://bugzilla.redhat.com/show_bug.cgi?id=518633)<sup>1497</sup>,

[BZ#515650](https://bugzilla.redhat.com/show_bug.cgi?id=515650)<sup>1498</sup>)

\* this update ensures that the snmpd daemon is able to process and respond to broadcast UDP requests. ([BZ#521175](https://bugzilla.redhat.com/show_bug.cgi?id=521175)<sup>1499</sup>)

\* header files contained within the net-snmp-devel package differed according to the architecture of the system, i386 or Itanium, they were installed on. Because net-snmp is a multilib package, this update moves architecture-dependent header files into separate files, thus allowing development packages for different architectures to be installed on the same system. ([BZ#521820](https://bugzilla.redhat.com/show_bug.cgi?id=521820)<sup>1500</sup>)

\* the libnetsnmp shared object library maintains cached data in the /usr/share/snmp/mibs/.index file. Because this file did not have the proper SELinux context, SELinux denied applications write access to this file. This update ensures that this .index file is properly labeled with the correct SELinux context so that applications are permitted to access it. ([BZ#523249](https://bugzilla.redhat.com/show_bug.cgi?id=523249)<sup>1501</sup>)

\* the snmpd daemon was unable to process requests to create a new User-Based Security Model (USM) view with Object ID components larger than 255. With this update, snmpd is able to create new USM views with all valid OIDs. ([BZ#527364](https://bugzilla.redhat.com/show_bug.cgi?id=527364)<sup>1502</sup>)

---

<sup>1494</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=504742](https://bugzilla.redhat.com/show_bug.cgi?id=504742)

<sup>1495</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=507528](https://bugzilla.redhat.com/show_bug.cgi?id=507528)

<sup>1496</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=514703](https://bugzilla.redhat.com/show_bug.cgi?id=514703)

<sup>1497</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=518633](https://bugzilla.redhat.com/show_bug.cgi?id=518633)

<sup>1498</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=515650](https://bugzilla.redhat.com/show_bug.cgi?id=515650)

<sup>1499</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=521175](https://bugzilla.redhat.com/show_bug.cgi?id=521175)

<sup>1500</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=521820](https://bugzilla.redhat.com/show_bug.cgi?id=521820)

<sup>1501</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=523249](https://bugzilla.redhat.com/show_bug.cgi?id=523249)

<sup>1502</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=527364](https://bugzilla.redhat.com/show_bug.cgi?id=527364)

\* SNMP applications such as `snmpget` and `snmpwalk` reported "truncating unsigned value to 32 bits" errors on 64-bit architectures when they received invalid SNMP responses from legacy systems. With this update, SNMP programs suppress these error messages when the received SNMP response can still be parsed. ([BZ#528164](#)<sup>1503</sup>)

\* the `snmpd` daemon assumed that network interface hardware addresses were always 6 bytes in length. Hardware such as InfiniBand network cards can have addresses of a different size, in which case `snmpd` reported "ioctl 35123 returned -1" to `syslog`. With this update, `snmpd` does not make the 6-byte assumption, and this error is no longer logged. ([BZ#543499](#)<sup>1504</sup>)

\* the `snmpd` daemon reported IP addresses in the `ipCidrRouteTable` object as 8 bytes on 64-bit hardware. This update ensures that `snmpd` reports IPv4 addresses as 4 bytes. ([BZ#547698](#)<sup>1505</sup>)

All SNMP users are advised to upgrade to these updated `net-snmp` packages, which resolve these issues and add these enhancements.

## 1.130. net-tools

### 1.130.1. RHBA-2009:1677: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2009:1677](#)<sup>1506</sup>

An updated `net-tools` package that fixes several bugs and corrects errors in the `arp` and `ifconfig` man pages is now available.

The `net-tools` package contains basic networking tools, including `ifconfig`, `netstat`, `route`, and others.

This updated `net-tools` package includes fixes for the following bugs:

\* the `OPTIONS` section of the `arp` man page includes documentation for the `-s` switch (used to manually create ARP address mapping entries). Entries supplied with this switch are permanently stored in the ARP cache if the `temp` flag is not specified and the original English man page notes this. The German man page, however, noted "so werden die erzeugten Einträge nicht dauerhaft... eingetragen", which is incorrect. This update corrects this, with the German man page now correctly noting "Der Eintrag wird permanent im ARP-Cache gespeichert" if the `temp` flag is not specified. ([BZ#322901](#)<sup>1507</sup>)

\* the `ifconfig` `"tunnel"` option creates a new Simple Internet Transition (SIT) or IPv6-in-IPv4 device and this option expects an IPv6-style address as a parameter. If an IPv4 address is used, the command fails. The `ifconfig` man page, however, listed the option and parameter as `"tunnel aa.bb.cc.dd"` which did not make it clear the IPv4 address must be provided in IPv6 notation. This update clarifies the man page notation. It now reads `"tunnel ::aa.bb.cc.dd"`, making it clear IPv6-style address notation is required. ([BZ#453918](#)<sup>1508</sup>)

---

<sup>1503</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=528164](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=528164)

<sup>1504</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=543499](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=543499)

<sup>1505</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=547698](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=547698)

<sup>1507</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=322901](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=322901)

<sup>1508</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=453918](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=453918)

\* running netstat with the "-o" switch adds information about working TCP timers to the command output. TCP timers for a connection can include "on", "off", "keepalive" and "timewait". When network load is very high (ie when the TCP Window Size is zero) the probe timer should be listed. Previously, however, "unkn-4" was presented instead. With this update, if the probe timer is working in the kernel, it will now, correctly, be listed in the output of "netstat -o". ([BZ#466845](#)<sup>1509</sup>)

\* when setting the MULTICAST mode on and off, ifconfig was showing an unnecessary "Warning: Interface [interface name] still in ALLMULTI mode." message. With this update, the message no longer presents. ([BZ#477876](#)<sup>1510</sup>)

\* a fixed length, 1024 byte buffer in the statistics.c:process\_fd() function caused "netstat -s" to fail with a "error parsing /proc/net/netstat: Success" error. The buffer has been increased to 2048 bytes and the command now displays summary statistics for each protocol as expected. ([BZ#493314](#)<sup>1511</sup>)

All net-tools users should install this updated package, which makes these corrections and addresses these issues.

## 1.131. NetworkManager

### 1.131.1. RHSA-2010:0108: Moderate security update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2010:0108](#)<sup>1512</sup>

Updated NetworkManager packages that fix two security issues are now available for Red Hat Enterprise Linux 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

NetworkManager is a network link manager that attempts to keep a wired or wireless network connection active at all times.

A missing network certificate verification flaw was found in NetworkManager. If a user created a WPA Enterprise or 802.1x wireless network connection that was verified using a Certificate Authority (CA) certificate, and then later removed that CA certificate file, NetworkManager failed to verify the identity of the network on the following connection attempts. In these situations, a malicious wireless network spoofing the original network could trick a user into disclosing authentication credentials or communicating over an untrusted network. ([CVE-2009-4144](#)<sup>1513</sup>)

An information disclosure flaw was found in NetworkManager's nm-connection-editor D-Bus interface. If a user edited network connection options using nm-connection-editor, a summary of those changes was broadcasted over the D-Bus message bus, possibly disclosing sensitive information (such as wireless network authentication credentials) to other local users. ([CVE-2009-4145](#)<sup>1514</sup>)

<sup>1509</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=466845](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=466845)

<sup>1510</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=477876](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=477876)

<sup>1511</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=493314](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=493314)

<sup>1513</sup> <https://www.redhat.com/security/data/cve/CVE-2009-4144.html>

<sup>1514</sup> <https://www.redhat.com/security/data/cve/CVE-2009-4145.html>

Users of NetworkManager should upgrade to these updated packages, which contain backported patches to correct these issues.

### 1.131.2. RHBA-2010:0263: bug fix update

Updated NetworkManager packages that resolve several issues are now available.

NetworkManager is a network link manager that attempts to keep a wired or wireless network connection active at all times.

These updated NetworkManager packages provide fixes for the following bugs:

\* creating a new wired connection which uses 802.1x security and then attempting to use that connection during the same desktop session resulted in NetworkManager being unable to establish that connection. As a workaround, logging out of the current desktop session and logging back in allowed the secure connection to be used. With this update, wired connections using 802.1x security can be used as soon as they are created. ([BZ#477061](#)<sup>1515</sup>)

\* due to a coding error, NetworkManager rejected WPA passkeys of exactly 63 ASCII characters in length, even though such a passkey is valid according to the standard. This was caused by a coding error which has been fixed in this update, thus correctly permitting 63-character passkeys. ([BZ#532723](#)<sup>1516</sup>)

\* NetworkManager failed to initialize certain Option NV mobile broadband (3G) devices. Much-improved support has been added for newer mobile broadband devices manufactured by Option NV, such as AT&T Quicksilver modems. ([BZ#536897](#)<sup>1517</sup>)

All users of NetworkManager are advised to upgrade to these updated packages, which resolve these issues.

## 1.132. newt

### 1.132.1. RHSA-2009:1463: Moderate security update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2009:1463](#)<sup>1518</sup>

Updated newt packages that fix one security issue are now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

Newt is a programming library for color text mode, widget-based user interfaces. Newt can be used to add stacked windows, entry widgets, checkboxes, radio buttons, labels, plain text fields, scrollbars, and so on, to text mode user interfaces.

---

<sup>1515</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=477061](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=477061)

<sup>1516</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=532723](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=532723)

<sup>1517</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=536897](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=536897)



A heap-based buffer overflow flaw was found in the way newt processes content that is to be displayed in a text dialog box. A local attacker could issue a specially-crafted text dialog box display request (direct or via a custom application), leading to a denial of service (application crash) or, potentially, arbitrary code execution with the privileges of the user running the application using the newt library. ([CVE-2009-2905](https://www.redhat.com/security/data/cve/CVE-2009-2905.html)<sup>1519</sup>)

Users of newt should upgrade to these updated packages, which contain a backported patch to correct this issue. After installing the updated packages, all applications using the newt library must be restarted for the update to take effect.

## 1.132.2. RHBA-2009:1482: bug fix update



### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2009:1482](https://bugzilla.redhat.com/show_bug.cgi?id=468046)<sup>1520</sup>

Updated newt packages that resolve several issues are now available.

Newt is a programming library for color text-mode, widget-based user interfaces. Newt can be used to add stacked windows, entry widgets, check boxes, radio buttons, labels, plain text fields, and so on, to text mode user interfaces.

These updated newt packages provide fixes for the following bugs:

\* the whiptail(1) man page was missing from the newt package, and is now included. ([BZ#456307](https://bugzilla.redhat.com/show_bug.cgi?id=456307)<sup>1521</sup>)

\* newt did not recognize the escape sequence "\E[Z" as the Shift+Tab key combination on VT320 terminals, and incorrectly interpreted it as "Escape". With these updated packages, newt correctly interprets "\E[Z" as Shift+Tab. ([BZ#468046](https://bugzilla.redhat.com/show_bug.cgi?id=468046)<sup>1522</sup>)

All users of newt are advised to upgrade to these updated packages, which resolve these issues.

## 1.133. nfs-utils

### 1.133.1. RHBA-2010:0284: bug fix update

An updated nfs-utils package that fixes two bugs is now available.

The nfs-utils package provides a daemon for the kernel NFS (Network File System) server and related tools, which provides better performance than the traditional Linux NFS server. This package also contains the mount.nfs, umount.nfs and showmount programs. Showmount queries the mount daemon on a remote host for information about the NFS server on the remote host. For example, showmount can display the clients which are mounted on that host.

This update addresses the following bugs:

\* nfsnobody == 4294967294 causes idmapd to stop responding. ([BZ#523285](https://bugzilla.redhat.com/show_bug.cgi?id=523285)<sup>1523</sup>)

<sup>1519</sup> <https://www.redhat.com/security/data/cve/CVE-2009-2905.html>

<sup>1521</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=456307](https://bugzilla.redhat.com/show_bug.cgi?id=456307)

<sup>1522</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=468046](https://bugzilla.redhat.com/show_bug.cgi?id=468046)

<sup>1523</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=523285](https://bugzilla.redhat.com/show_bug.cgi?id=523285)



\* inconsistent default anonuid/anongid values. ([BZ#497551](#)<sup>1524</sup>)

All nfs-utils users should install this updated package, which addresses these issues.

### 1.134. nspluginwrapper

#### 1.134.1. RHBA-2010:0187: bug fix update

An updated nspluginwrapper package that fixes various bugs is now available.

nspluginwrapper is a utility which allows 32-bit plug-ins to run in a 64-bit browser environment (a common example is Adobe's browser plug-in for presenting proprietary Flash files embedded in web pages). It includes the plug-in viewer and a tool for managing plug-in installations and updates.

The nspluginwrapper package has been upgraded to version 1.3.0-8.el5.

This update contains fixes for the following bugs:

\* The nspluginwrapper package contained a bug that restricted expected functionality with PDF files viewed in the Firefox web browser. Limitations included the inability to search a PDF document because the Find bar was unable to get focus to enable a user to input a search term and unable to use the keyboard shortcuts F8, Ctrl+Shift+F8 and Ctrl+E. A user is now able to search a PDF document loaded in Firefox and all predefined keyboard shortcuts work correctly. ([BZ#435838](#)<sup>1525</sup>, [BZ#455218](#)<sup>1526</sup>)

\* When the previous version of the nspluginwrapper package was used with Adobe Flash 10 and Firefox was run from the terminal window, critical error messages would present in the terminal even though the software worked as expected. The error messages do not appear in the terminal window with this latest upgrade. ([BZ#466547](#)<sup>1527</sup>)

\* If the umask of the user that invoked /usr/bin/mozilla-plugin-config was 0077, the files in /usr/lib/mozilla/plugins-wrapped/ would be given permissions based on the users umask. This could have lead to the files becoming unreadable. With this package update, nspluginwrapper does not use the umask or group inherited from the invoking user. ([BZ#521948](#)<sup>1528</sup>, [BZ#523814](#)<sup>1529</sup>)

Users of nspluginwrapper should upgrade to this updated package, which resolves these issues.

### 1.135. nss\_ldap

#### 1.135.1. RHBA-2009:1527: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1527](#)<sup>1530</sup>

---

<sup>1524</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=497551](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=497551)

<sup>1525</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=435838](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=435838)

<sup>1526</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=455218](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=455218)

<sup>1527</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=466547](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=466547)

<sup>1528</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=521948](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=521948)

<sup>1529</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=523814](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=523814)

An updated nss\_ldap package is now available for Red Hat Enterprise Linux 5.

The nss\_ldap package includes two LDAP access clients: nss\_ldap and pam\_ldap. nss\_ldap is a plugin for the standard C library which allows applications to look up information about users and groups using a directory server. The pam\_ldap module is a Pluggable Authentication Module (PAM) which provides for authentication, authorization and password changing against LDAP servers.

This update fixes the following bug in the nss\_ldap module:

\* a NULL value was incorrectly assigned to an ldap\_parse\_result argument if the bind operation timed out. Consequently, if the nss\_ldap module was configured to encrypt traffic to the directory server using the "ssl start\_tls" option and TLS negotiation took longer than the "bind\_timelimit" value set in /etc/ldap.conf, the client module would crash with an Assertion error. With this update, the ldap\_parse\_result argument is not set to NULL if the bind operation times out and the Assertion error no longer occurs. ([BZ#529376](https://bugzilla.redhat.com/show_bug.cgi?id=529376)<sup>1531</sup>)

Note: The default bind\_timelimit is 30 seconds and this bug did not normally trigger unless the value was set to less than this default. Further, it was possible to workaround this issue by increasing the bind\_timelimit (for example, to 60 seconds). This only masked the underlying issue, however.

All nss\_ldap users are advised to upgrade to this updated package, which resolves this issue.

## 1.135.2. RHBA-2010:0260: bug fix update

An updated nss\_ldap package that fixes various bugs is now available.

The nss\_ldap package includes two LDAP access clients: nss\_ldap and pam\_ldap. nss\_ldap is a plugin for the standard C library which allows applications to look up information about users and groups using a directory server. The pam\_ldap module is a Pluggable Authentication Module (PAM) which provides for authentication, authorization and password changing against LDAP servers.

This package addresses the following bugs:

\* The nss\_ldap package did not support case sensitive text. This could cause group membership not to be matched to the users. To correct this name resolution for users, group, and shadow information can now be forced to be performed in a case sensitive manner by setting "nss\_check\_case yes" in /etc/ldap.conf. The default setting remains as "nss\_check\_case no". This fix results in group membership being matched to the correct users. ([BZ#518911](https://bugzilla.redhat.com/show_bug.cgi?id=518911)<sup>1532</sup>)

\* When running commands, sometimes the nss\_ldap library would produce assertion errors, leading to application failure. To fix this bug the nss\_ldap package has been modified to allow for bind\_timeout in /etc/ldap.conf to be set to a low value (for example, 2). If the bind performed does time out it now performs a debug request instead of producing assertion errors. ([BZ#499302](https://bugzilla.redhat.com/show_bug.cgi?id=499302)<sup>1533</sup>)

\* By setting the value 'bind\_policy soft' in the /etc/ldap.conf file and configuring hostname resolution to only use 'ldap', it becomes impossible to resolve any information about the server without first contacting it. This meant that when using the command getent -s 'ldap' passwd, a segmentation fault would occur. This updated nss\_ldap package ensures that no segmentation fault occurs, however the correct way to access the server information in the outlined case would be to use the command getent -s 'passwd:ldap' passwd. ([BZ#448883](https://bugzilla.redhat.com/show_bug.cgi?id=448883)<sup>1534</sup>)

<sup>1531</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=529376](https://bugzilla.redhat.com/show_bug.cgi?id=529376)

<sup>1532</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=518911](https://bugzilla.redhat.com/show_bug.cgi?id=518911)

<sup>1533</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=499302](https://bugzilla.redhat.com/show_bug.cgi?id=499302)

<sup>1534</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=448883](https://bugzilla.redhat.com/show_bug.cgi?id=448883)

\* When LDAP was listed before DNS in the `nsswitch.conf` file and the hostname was not in the `/etc/hosts` file, the `nss_ldap` package caused segmentation faults. Segmentation faults occurred with `nscd`, `getent` and any process that used the library when communicating with the secondary OpenLDAP servers. This package update ensures that `nss_ldap` does not produce any segmentation faults when interacting with OpenLDAP servers. ([BZ#472920](#)<sup>1535</sup>)

\* The `nss_ldap` package would write to a socket that was not connected to an LDAP server. This resulted in an EPIPE error being returned and all shell commands ceasing to work when logged in as an LDAP user. To fix this bug the `sigpipe` is now unblocked when closing the connection in the `child` element. This allows for shell commands to continue to function. ([BZ#454315](#)<sup>1536</sup>)

All `nss_ldap` users are advised to upgrade to this updated package, which resolves these issue.

## 1.136. numactl

### 1.136.1. RHBA-2010:0319: bug fix update

An updated `numactl` package that fixes a bug is now available

`numactl` adds simple Non-Uniform Memory Access (NUMA) policy support. It consists of a `numactl` program to run other programs with a specific NUMA policy and a `libnuma` to do allocations with NUMA policy in applications.

This updated package addresses the following issue:

\* `libvirt` tools reported unnecessary warning messages to `stderr` during execution. This caused problems with scripts calling these tools. Those warning messages have been repressed, and the scripts are no longer affected. ([BZ#555805](#)<sup>1537</sup>)

Users are advised to upgrade to this updated `numactl` package which resolves this issue.

### 1.136.2. RHBA-2009:1626: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2009:1626](#)<sup>1538</sup>

Updated `numactl` packages that resolve several issues are now available.

`numactl` is Simple NUMA policy support. It consists of a `numactl` program to run other programs with a specific NUMA policy, and the `libnuma` library, which performs allocations with NUMA policy in applications.

These updated `numactl` packages provide fixes for the following bugs:

---

<sup>1535</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=472920](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=472920)

<sup>1536</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=454315](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=454315)

<sup>1537</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=555805](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=555805)

\* systems with NUMA nodes which were not ordered contiguously caused numactl to return incorrect and therefore invalid NUMA data. With this update, numactl shows correct and valid data for systems with NUMA nodes which are discontinuous in addition to those which are contiguous. ([BZ#491689](#)<sup>1539</sup>)

\* the "numactl" command possesses an '-H' short option that corresponds to the long option, '--hardware', which is used to show the inventory of available nodes on the system. However, numactl did not recognize the short '-H' option. With this update, numactl now recognizes the '-H' option, which once again has the same affect as '--hardware'. ([BZ#502241](#)<sup>1540</sup>)

All users of numactl are advised to upgrade to these updated packages, which resolve these issues.

## 1.137. openCryptoki

### 1.137.1. RHBA-2009:1685: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1685](#)<sup>1541</sup>

Updated openCryptoki packages that resolve several issues are now available.

The openCryptoki package contains version 2.11 of the PKCS#11 API, implemented for IBM Cryptocards. This package includes support for the IBM 4758 Cryptographic CoProcessor (with the PKCS#11 firmware loaded), the IBM eServer Cryptographic Accelerator (FC 4960 on IBM eServer System p), the IBM Crypto Express2 (FC 0863 or FC 0870 on IBM System z), the IBM CP Assist for Cryptographic Function (FC 3863 on IBM System z).

These updated openCryptoki packages provide fixes for the following bugs:

\* after initializing a hardware cryptographic token, attempting to unwrap an AES key failed and caused openCryptoki to return a "CKR\_TEMPLATE\_INCOMPLETE" error code. With this update, AES key unwrapping now succeeds as expected. ([BZ#540471](#)<sup>1542</sup>)

\* the openCryptoki API enables programs to offload the computation of the message authentication code (MAC) to the Central Processor Assist for Cryptographic Function (CPACF) of cryptographic hardware. When using PKCS#11 for the acceleration of cryptographic instructions, openCryptoki returned an error code of "411", indicating that the MAC was unable to be verified. With this update, the MAC is now computed successfully after being offloaded to the CPACF. ([BZ#540474](#)<sup>1543</sup>)

\* openCryptoki was not properly recognizing that secure-key crypto support was installed, and so the "CCA" token was not being enabled for use. ([BZ#545379](#)<sup>1544</sup>)

All users of openCryptoki are advised to upgrade to these updated packages, which resolve these issues.

<sup>1539</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=491689](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=491689)

<sup>1540</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=502241](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=502241)

<sup>1542</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=540471](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=540471)

<sup>1543</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=540474](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=540474)

<sup>1544</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=545379](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=545379)

### 1.138. openais

#### 1.138.1. RHBA-2009:1474: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1474](#)<sup>1545</sup>

An updated openais package that fixes a bug is now available for Red Hat Enterprise Linux 5.4.

The Application Interface Specification (AIS) is an API and set of policies for developing applications that maintain service during faults. The OpenAIS Standards Based Cluster Framework is an OSI-certified implementation of the Service Availability Forum AIS. The openais package contains the openais executive, openais service handlers, default configuration files and init script.

This update addresses the following issue:

\* an invalid assertion caused MTUs of 9000 bytes to generate a SIGABRT signal and dump core when inside totem running heavy loads. With this update, the assertion has been corrected (and the MTU increased to 10000 bytes). ([BZ#521098](#)<sup>1546</sup>)

All openais users should install this update which fixes this bug.

#### 1.138.2. RHBA-2010:0180: bug fix update

Updated openais packages that fix several defects are now available for Red Hat Enterprise Linux 5.5.

The Open Application Interface Specification (OpenAIS) is an API and a set of policies for developing applications that maintain service during faults. The OpenAIS Standards-Based Cluster Framework is an OSI-certified implementation of the Service Availability Forum AIS. The openais packages contain the openais executive, openais service handlers, default configuration files, and init script.

This update addresses the following issues:

\* Resolve a segfault if the ais group doesn't exist. Note the ais group is installed by the package but may be removed by the user later. This resolution prints an error in that condition. ([BZ#509180](#)<sup>1547</sup>)

\* Properly shut down service engines when the INTR signal or QUIT signal is sent to the aisexec process. ([BZ#526069](#)<sup>1548</sup>)

\* Resolve a race condition in the cpg service which could result in failures during recovery of cpg services. ([BZ#474400](#)<sup>1549</sup>)

\* A random error code was returned by saCkptCheckpointOpen if the internal IPC operation failed. Now the proper SA\_AIS\_ERR\_LIBRARY error code is returned in this condition. ([BZ#520164](#)<sup>1550</sup>)

---

<sup>1546</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=521098](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=521098)

<sup>1547</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=509180](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=509180)

<sup>1548</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=526069](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=526069)

<sup>1549</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=474400](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=474400)

<sup>1550</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=520164](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=520164)

- \* An invalid assertion caused MTUs of 9000 bytes to generate a SIGABRT signal and dump core when inside totem running heavy loads. With this update, the assertion has been corrected (and the MTU increased to 10000 bytes). ([BZ#520012](https://bugzilla.redhat.com/show_bug.cgi?id=520012)<sup>1551</sup>)
- \* Resolve a problem where checkpoint iteration and discovery can happen during synchronization of new data structures. This results in the GFS POSIX locking feature appearing to leave leftover locks on nodes that no longer exist. ([BZ#515159](https://bugzilla.redhat.com/show_bug.cgi?id=515159)<sup>1552</sup>)
- \* Resolve a stack overflow that results in a stack protector assertion. ([BZ#525280](https://bugzilla.redhat.com/show_bug.cgi?id=525280)<sup>1553</sup>)
- \* Resolve a defect when calling saCmTrackStart more than one time can trigger a segfault in library clients to the clm service. ([BZ#529054](https://bugzilla.redhat.com/show_bug.cgi?id=529054)<sup>1554</sup>)
- \* Resolve a defect where cpg can use a variable after it has been freed. ([BZ#540267](https://bugzilla.redhat.com/show_bug.cgi?id=540267)<sup>1555</sup>)
- \* Resolve a defect where the bindnetaddr does not follow the specifications outlined by the man pages for operation because it uses the interface's broadcast address instead of its local address for binding. ([BZ#540490](https://bugzilla.redhat.com/show_bug.cgi?id=540490)<sup>1556</sup>)
- \* Resolve a defect where originating 206 messages in the recovery phase triggers totem to block until a processor is stopped or started. ([BZ#544680](https://bugzilla.redhat.com/show_bug.cgi?id=544680)<sup>1557</sup>)
- \* Resolve a defect where a buffer overflow can occur in a string buffer used when the "debug: on" option is used in the configuration. ([BZ#544682](https://bugzilla.redhat.com/show_bug.cgi?id=544682)<sup>1558</sup>)
- \* Resolve a defect where an internal totem operating flag is not set properly. ([BZ#545151](https://bugzilla.redhat.com/show_bug.cgi?id=545151)<sup>1559</sup>)
- \* Resolve a defect where an invalid assertion in single-node operation can trigger an assertion. ([BZ#547828](https://bugzilla.redhat.com/show_bug.cgi?id=547828)<sup>1560</sup>)
- \* Resolve a defect where the IPC limit was 477k instead of 1MB as it should be. ([BZ#515590](https://bugzilla.redhat.com/show_bug.cgi?id=515590)<sup>1561</sup>)
- \* Resolve a defect where IPC would indicate the outbound ipc queue was empty when the IPC queue is fully consumed by data. ([BZ#560313](https://bugzilla.redhat.com/show_bug.cgi?id=560313)<sup>1562</sup>)
- \* Resolve a defect where errant code calls pthread\_cond\_wait in an atexit() handler, resulting in lockup of the aisexec daemon 1% of the time on shutdown. ([BZ#566467](https://bugzilla.redhat.com/show_bug.cgi?id=566467)<sup>1563</sup>)

All openais users should install this update, which fixes these bugs.

---

<sup>1551</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=520012](https://bugzilla.redhat.com/show_bug.cgi?id=520012)

<sup>1552</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=515159](https://bugzilla.redhat.com/show_bug.cgi?id=515159)

<sup>1553</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=525280](https://bugzilla.redhat.com/show_bug.cgi?id=525280)

<sup>1554</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=529054](https://bugzilla.redhat.com/show_bug.cgi?id=529054)

<sup>1555</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=540267](https://bugzilla.redhat.com/show_bug.cgi?id=540267)

<sup>1556</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=540490](https://bugzilla.redhat.com/show_bug.cgi?id=540490)

<sup>1557</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=544680](https://bugzilla.redhat.com/show_bug.cgi?id=544680)

<sup>1558</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=544682](https://bugzilla.redhat.com/show_bug.cgi?id=544682)

<sup>1559</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=545151](https://bugzilla.redhat.com/show_bug.cgi?id=545151)

<sup>1560</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=547828](https://bugzilla.redhat.com/show_bug.cgi?id=547828)

<sup>1561</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=515590](https://bugzilla.redhat.com/show_bug.cgi?id=515590)

<sup>1562</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=560313](https://bugzilla.redhat.com/show_bug.cgi?id=560313)

<sup>1563</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=566467](https://bugzilla.redhat.com/show_bug.cgi?id=566467)

## 1.139. OpenIPMI

### 1.139.1. RHBA-2009:1487: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1487](#)<sup>1564</sup>

Updated OpenIPMI packages that resolve an issue are now available

OpenIPMI (Intelligent Platform Management Interface) provides command line tools and utilities to access platform information, allowing system administrators to monitor system health and manage systems.

This update addresses the following problem:

\* some IPMI-enabled hardware uses UDP ports 623 (ASF Remote Management and Control Protocol) and 664 (ASF Secure Remote Management and Control Protocol), which can conflict with other traffic on these ports. The previous OpenIPMI release added a configuration file `-- /etc/xinetd.d/rmcp --` for a dummy rmcp service and introduced an xinetd service dependency to bind UDP ports 623 and 664 and prevent other services from using them.

Because the xinetd service is started by default, the update resulted in a new xinetd daemon running on systems after OpenIPMI was updated. This daemon is not necessary for OpenIPMI operation.

This update removes the dependency on xinetd but leaves the dummy rmcp service configuration file in place. ([BZ#527474](#)<sup>1565</sup>)

All OpenIPMI users are advised to upgrade to these updated packages which remove this dependency. If the previous OpenIPMI update started an unnecessary xinetd service, stopping and removing this service is also recommended.

### 1.139.2. RHBA-2009:1629: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2009:1629](#)<sup>1566</sup>

Updated OpenIPMI packages that resolve several issues are now available.

OpenIPMI (Intelligent Platform Management Interface) provides command line tools and utilities to access platform information, allowing system administrators to monitor system health and manage systems.

This update addresses the following problem:

---

<sup>1565</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=527474](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=527474)



\* the ipmitool man page did not contain descriptions of the "hpm" and "fwum" commands. In addition, the man page did not document the "noguard" parameter of the "sol set" command. These commands and parameters are properly described in the updated ipmitool man page. ([BZ#514215](#)<sup>1567</sup>, [BZ#513609](#)<sup>1568</sup>)

\* the ipmievd init script did not properly implement the "condrestart" action. This could result in the ipmievd daemon not being restarted after a package update. The condrestart action in the ipmievd init script is fixed in this update. ([BZ#532445](#)<sup>1569</sup>)

\* on some IPMI-enabled hardware, especially hardware with an on-board IPMI watchdog supported by the i6300esb driver or an Intel TCO Watchdog Timer device supported by the iTCO\_wdt driver, the /dev/watchdog device is created directly by the kernel during boot. If the ipmi service with enabled watchdog was then started, the init script did not recognize the existing watchdog device and tried to instantiate new one. This resulted in an error which was not reported to the user. The updated ipmi init script now returns a "/dev/watchdog already exists [FAILED]" message in this circumstance. ([BZ#514678](#)<sup>1570</sup>)

\* some IPMI-enabled hardware uses UDP ports 623 (ASF Remote Management and Control Protocol) and 664 (ASF Secure Remote Management and Control Protocol), which can conflict with other traffic on these ports. The previous OpenIPMI release added a configuration file -- /etc/xinetd.d/rmcp -- for a dummy rmcp service and introduced an xinetd service dependency to bind UDP ports 623 and 664 and prevent other services from using them.

Because the xinetd service is started by default, the update resulted in a new xinetd daemon running on systems after OpenIPMI was updated. This daemon is not necessary for OpenIPMI operation.

This update removes the dependency on xinetd but leaves the dummy rmcp service configuration file in place. ([BZ#522524](#)<sup>1571</sup>)

All OpenIPMI users are advised to upgrade to these updated packages. If the previous OpenIPMI update started an unnecessary xinetd service, stopping and removing this service is also recommended.

## 1.140. openib

### 1.140.1. RHBA-2010:0292: bug fix and enhancement update

Updated openib packages that fix various bugs and add various enhancements are now available.

Red Hat Enterprise Linux includes a collection of Infiniband and iWARP utilities, libraries and development packages for writing applications that use Remote Direct Memory Access (RDMA) technology.

The following general upgrade has been performed:

\* this update brings a number of packages in line with their latest upstream versions. ([BZ#518218](#)<sup>1572</sup>)

<sup>1567</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=514215](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=514215)

<sup>1568</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=513609](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=513609)

<sup>1569</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=532445](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=532445)

<sup>1570</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=514678](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=514678)

<sup>1571</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=522524](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=522524)

<sup>1572</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=518218](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=518218)



Also, these updated packages fix the following bugs:

- \* even simple test code could not be compiled using mvapich if mvapich was installed but certain other libraries were not. To correct this, the mvapich rpm now Requires all libraries necessary to build an mpi program. ([BZ#479940](https://bugzilla.redhat.com/show_bug.cgi?id=479940)<sup>1573</sup>, [BZ#568449](https://bugzilla.redhat.com/show_bug.cgi?id=568449)<sup>1574</sup>)
- \* when running openmpi jobs, many warnings would present related to udapl. The issue is corrected by removing udapl support from openmpi. ([BZ#479941](https://bugzilla.redhat.com/show_bug.cgi?id=479941)<sup>1575</sup>, [BZ#526138](https://bugzilla.redhat.com/show_bug.cgi?id=526138)<sup>1576</sup>, [BZ#543453](https://bugzilla.redhat.com/show_bug.cgi?id=543453)<sup>1577</sup>)
- \* openmpi did not support the latest Chelsio devices. This release corrects that. ([BZ#515567](https://bugzilla.redhat.com/show_bug.cgi?id=515567)<sup>1578</sup>)
- \* a bug in IPoIB bonding could cause the kernel to panic during the reboot of a system. The openibd init script has been modified to correct this bug. ([BZ#540992](https://bugzilla.redhat.com/show_bug.cgi?id=540992)<sup>1579</sup>)
- \* in the update to openmpi-1.3.2, upstream changed the default value of SGE support from enabled to disabled, which caused Red Hat's version of the openmpi package to regress. These updated packages restore SGE support in Red Hat's openmpi packages. ([BZ#541660](https://bugzilla.redhat.com/show_bug.cgi?id=541660)<sup>1580</sup>)
- \* the srp\_daemon.conf configuration file was not in the "/etc" directory where srp\_daemon requires it to be. During installation the srp\_daemon.conf file was being placed in the incorrect directory of "/etc/ofed". This issue is fixed by ensuring the srp\_daemon.conf file is placed in the "/etc" directory during installation. ([BZ#552915](https://bugzilla.redhat.com/show_bug.cgi?id=552915)<sup>1581</sup>)
- \* a regression was introduced in openmpi-1.3.3-6 that caused allreduce to hang. This regression is now corrected with these updated packages and allreduce functions as expected. ([BZ#555159](https://bugzilla.redhat.com/show_bug.cgi?id=555159)<sup>1582</sup>)
- \* a pseudo requirement has been added to the libibverbs package so that it will automatically pull in the various libibverbs driver packages when using yum to install libibverbs. ([BZ#559789](https://bugzilla.redhat.com/show_bug.cgi?id=559789)<sup>1583</sup>)
- \* Libmlx4 was missing device IDs that were present in the Red Hat Enterprise Linux kernel. The missing device IDs have now been added to libmlx4. These IDs are for MT26438 and MT26488. ([BZ#569175](https://bugzilla.redhat.com/show_bug.cgi?id=569175)<sup>1584</sup>)

the following enhancements were also added:

- \* Openmpi now supports iWARP devices. ([BZ#515565](https://bugzilla.redhat.com/show_bug.cgi?id=515565)<sup>1585</sup>)
- \* the OpenFabrics Alliance (OFED) drivers which support Mellanox MT25408 ConnectX series Infiniband devices were added. ([BZ#511190](https://bugzilla.redhat.com/show_bug.cgi?id=511190)<sup>1586</sup>)

All openib users should upgrade to these updated packages which resolves these issues and adds these enhancements.

---

<sup>1573</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=479940](https://bugzilla.redhat.com/show_bug.cgi?id=479940)

<sup>1574</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=568449](https://bugzilla.redhat.com/show_bug.cgi?id=568449)

<sup>1575</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=479941](https://bugzilla.redhat.com/show_bug.cgi?id=479941)

<sup>1576</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=526138](https://bugzilla.redhat.com/show_bug.cgi?id=526138)

<sup>1577</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=543453](https://bugzilla.redhat.com/show_bug.cgi?id=543453)

<sup>1578</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=515567](https://bugzilla.redhat.com/show_bug.cgi?id=515567)

<sup>1579</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=540992](https://bugzilla.redhat.com/show_bug.cgi?id=540992)

<sup>1580</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=541660](https://bugzilla.redhat.com/show_bug.cgi?id=541660)

<sup>1581</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=552915](https://bugzilla.redhat.com/show_bug.cgi?id=552915)

<sup>1582</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=555159](https://bugzilla.redhat.com/show_bug.cgi?id=555159)

<sup>1583</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=559789](https://bugzilla.redhat.com/show_bug.cgi?id=559789)

<sup>1584</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=569175](https://bugzilla.redhat.com/show_bug.cgi?id=569175)

<sup>1585</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=515565](https://bugzilla.redhat.com/show_bug.cgi?id=515565)

<sup>1586</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=511190](https://bugzilla.redhat.com/show_bug.cgi?id=511190)

## 1.141. openldap

### 1.141.1. RHSA-2010:0198: Moderate security and bug fix update

Updated openldap packages that fix one security issue and several bugs are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

OpenLDAP is an open source suite of LDAP (Lightweight Directory Access Protocol) applications and development tools.

A flaw was found in the way OpenLDAP handled NUL characters in the CommonName field of X.509 certificates. An attacker able to get a carefully-crafted certificate signed by a trusted Certificate Authority could trick applications using OpenLDAP libraries into accepting it by mistake, allowing the attacker to perform a man-in-the-middle attack. ([CVE-2009-3767](#)<sup>1587</sup>)

This update also fixes the following bugs:

\* the ldap init script did not provide a way to alter system limits for the slapd daemon. A variable is now available in "/etc/sysconfig/ldap" for this option. ([BZ#527313](#)<sup>1588</sup>)

\* applications that use the OpenLDAP libraries to contact a Microsoft Active Directory server could crash when a large number of network interfaces existed. This update implements locks in the OpenLDAP library code to resolve this issue. ([BZ#510522](#)<sup>1589</sup>)

\* when slapd was configured to allow client certificates, approximately 90% of connections froze because of a large CA certificate file and slapd not checking the success of the SSL handshake. ([BZ#509230](#)<sup>1590</sup>)

\* the OpenLDAP server would freeze for unknown reasons under high load. These packages add support for accepting incoming connections by new threads, resolving the issue. ([BZ#507276](#)<sup>1591</sup>)

\* the compat-openldap libraries did not list dependencies on other libraries, causing programs that did not specifically specify the libraries to fail. Detection of the Application Binary Interface (ABI) in use on 64-bit systems has been added with this update. ([BZ#503734](#)<sup>1592</sup>)

\* the OpenLDAP libraries caused applications to crash due to an unprocessed network timeout. A timeval of -1 is now passed when NULL is passed to LDAP. ([BZ#495701](#)<sup>1593</sup>)

\* slapd could crash on a server under heavy load when using rwm overlay, caused by freeing non-allocated memory during operation cleanup. ([BZ#495628](#)<sup>1594</sup>)

---

<sup>1587</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3767.html>

<sup>1588</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=527313](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=527313)

<sup>1589</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=510522](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=510522)

<sup>1590</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=509230](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=509230)

<sup>1591</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=507276](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=507276)

<sup>1592</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=503734](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=503734)

<sup>1593</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=495701](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=495701)

<sup>1594</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=495628](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=495628)

- \* the ldap init script made a temporary script in "/tmp/" and attempted to execute it. Problems arose when "/tmp/" was mounted with the noexec option. The temporary script is no longer created. ([BZ#483356](#)<sup>1595</sup>)
- \* the ldap init script always started slapd listening on ldap:/// even if instructed to listen only on ldaps://. By correcting the init script, a user can now select which ports slapd should listen on. ([BZ#481003](#)<sup>1596</sup>)
- \* the slapd manual page did not mention the supported options -V and -o. ([BZ#468206](#)<sup>1597</sup>)
- \* slapd.conf had a commented-out option to load the syncprov.la module. Once un-commented, slapd crashed at start-up because the module had already been statically linked to OpenLDAP. This update removes "moduleload syncprov.la" from slapd.conf, which resolves this issue. ([BZ#466937](#)<sup>1598</sup>)
- \* the migrate\_automount.pl script produced output that was unsupported by autofs. This is corrected by updating the output LDIF format for automount records. ([BZ#460331](#)<sup>1599</sup>)
- \* the ldap init script uses the TERM signal followed by the KILL signal when shutting down slapd. Minimal delay between the two signals could cause the LDAP database to become corrupted if it had not finished saving its state. A delay between the signals has been added via the "STOP\_DELAY" option in "/etc/sysconfig/ldap". ([BZ#452064](#)<sup>1600</sup>)
- \* the migrate\_passwd.pl migration script had a problem when number fields contained only a zero. Such fields were considered to be empty, leading to the attribute not being set in the LDIF output. The condition in dump\_shadow\_attributes has been corrected to allow for the attributes to contain only a zero. ([BZ#113857](#)<sup>1601</sup>)
- \* the migrate\_base.pl migration script did not handle third level domains correctly, creating a second level domain that could not be held by a database with a three level base. This is now allowed by modifying the migrate\_base.pl script to generate only one domain. ([BZ#104585](#)<sup>1602</sup>)

Users of OpenLDAP should upgrade to these updated packages, which resolve these issues.

## 1.142. openmotif

### 1.142.1. RHBA-2010:0132: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2010:0132](#)<sup>1603</sup>

Updated openmotif packages that resolve several issues are now available.

<sup>1595</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=483356](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=483356)

<sup>1596</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=481003](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=481003)

<sup>1597</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=468206](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=468206)

<sup>1598</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=466937](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=466937)

<sup>1599</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=460331](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=460331)

<sup>1600</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=452064](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=452064)

<sup>1601</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=113857](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=113857)

<sup>1602</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=104585](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=104585)

The openmotif packages include the Motif shared libraries needed to run applications which are dynamically linked against Motif, as well as mwm, the Motif Window Manager.

These updated openmotif packages provide fixes for the following bugs:

\* redisplaying a Label or LabelGadget widget could have caused a BadDrawable X error and resulted in an invisible label. This update resolves the issue with unspecified pixmaps so that labels do not become invisible and BadDrawable errors are not incurred. ([BZ#569906](#)<sup>1604</sup>)

\* selecting an item in a MultiList widget resulted in that item becoming invisible due to the same color being used for both foreground and background colors. The same problem occurred with "insensitive" labels, buttons, icons and list entries. With this update, foreground and background colors in widgets have been differentiated so that they do not become invisible during operation. ([BZ#569907](#)<sup>1605</sup>)

\* attempting to use a keyboard accelerator such as Ctrl+S failed to achieve the intended effect when the Caps Lock, Scroll Lock or NumLock keys were activated. This was caused by missing support for the X11R6 modifiers scheme. Support for the modifiers scheme has been implemented in this update so that keyboard accelerators can be used as expected even when modifiers such as Caps Lock, Scroll Lock or NumLock have been activated. ([BZ#569908](#)<sup>1606</sup>)

All users of openmotif are advised to upgrade to these updated packages, which resolve these issues.

## 1.143. openoffice.org

### 1.143.1. RHBA-2010:0274: bug fix and enhancement update

**OpenOffice.org** is a multi-platform office productivity suite. It includes the key desktop applications, such as a word processor, spreadsheet, presentation manager, formula editor and drawing program, with a user interface and feature set similar to other office suites. Sophisticated and flexible, **OpenOffice.org** also works transparently with a variety of file formats, including Microsoft Office.

These updated packages fix the following bugs:

- a nested table would be removed from the defined nesting structure when rendered in **Web Layout** view causing **OpenOffice.org** to crash. A patch has been applied to ensure the correct rendering of nested tables. ([BZ#469157](#)) ([BZ#469157](#)<sup>1607</sup>)
- using **OpenOffice.org Impress** in a dual monitor configuration and selecting **Slide Show** → **Slide Show** would cause the application to crash as the application was configured to return a default screen. A patch has been applied to detect and return the monitor upon which the slide show will be displayed. ([BZ#476949](#)<sup>1608</sup>)
- when saving a html document containing cells which are merged across rows, **OpenOffice.org Writer** would insert an additional cell in each row of the spanned set. When the document was rendered, the cells would appear to be misaligned due to the creation of the additional cells. A patch has been applied to retain the original table row span configuration. ([BZ#491357](#)<sup>1609</sup>)
- enabling the **Mozilla** plugin in **OpenOffice.org** and opening a **.odt** file in **Firefox** would generate a segmentation fault, causing **Firefox** to crash on x86\_64 architectures. A patch has been applied

<sup>1604</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=569906](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=569906)

<sup>1605</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=569907](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=569907)

<sup>1606</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=569908](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=569908)

to define the `uint32` and `int32` variables as the appropriate type of `int` or `long` depending on the architecture. ([BZ#496033](#)<sup>1610</sup>)

- when performing an **Edit** → **Find & Replace** operation in **OpenOffice.org Impress**, the **Find All** button was visible but inactive. A patch has been applied to remove the **Find All** button from the interface as this is not a supported **OpenOffice.org Impress** feature. ([BZ#504109](#)<sup>1611</sup>)
- when attempting to merge a `.sxi` or `.odt` file into an **OpenOffice.org Calc** document, the application would crash due to the `SfxMedium* pMed` pointer in `ScDocShell::DialogClosedHdl()` being set to **NULL**. A patch has been applied to the `docsh4.cxx` file to test the state of this variable prior to affecting the merge. ([BZ#504551](#)<sup>1612</sup>)
- when using **OpenOffice.org Calc** with spell check enabled, if a misspelt word was entered in a cell and the **Edit** → **Repeat:Insert** operation was attempted from within a new cell, the misspelt word would not be inserted. The `viewfunc.cxx` file has been updated to ensure that the insert operation is functional even if the original cell contents are misspelt. ([BZ#504967](#)<sup>1613</sup>)
- in **OpenOffice.org Calc**, the **Data** → **Group and Outline** → **AutoOutline** command would not work for any cell that contained a formula specifying a cell range as a list (for example: `=SUM(A1;A2;A3)`). To fix this bug the `cell.hxx` file has been modified to simplify a list range (for example: the list `A2;A1;A3` would become `A1:A3`). By condensing the list, the **Data** → **Group and Outline** → **AutoOutline** command now works as expected. ([BZ#504971](#)<sup>1614</sup>)
- building **RPMs** for **OpenOffice.org** would fail when a **Java** version above version 1.4 was installed. This occurred because the **ANT** scripts used to build some of the components were not configured to generate version 1.4 compatible bytecode upon which **OpenOffice.org** is dependent. This bug has since been fixed by enforcing **RPMs** to be built with the **GNU Compiler for Java** (GCJ) or the **Eclipse Compiler for Java** (EJC). GJC specific options have been omitted as these are not recognized by EJC. This ensures that **OpenOffice.org RPMs** are generated without error when using the `rpmbuild` command. ([BZ#506036](#)<sup>1615</sup>)
- when printing, **OpenOffice.org** would sometimes crash. This was due to the code that processes Postscript Printer Description (PPD) keys from **CUPS** inserting a value of **None** as the first value for each newly inserted key. Under these circumstances the second insertion returns a **NULL** pointer and the following statement causes the crash by dereferencing the pointer. To correct this bug the `jobset.cxx` file has been modified to only insert a value of **None** as the first value for each newly inserted key if it is not already present. ([BZ#515488](#)<sup>1616</sup>)
- when zooming in over 128% on a document in the **OpenOffice.org Writer**, any inserted note would no longer be viewable. By upgrading the **OpenOffice.org** suite to 3.1.1-19.5 this issue is no longer presented. ([BZ#521006](#)<sup>1617</sup>)
- bulleted lists in an **OpenOffice.org Writer** version 3 document would not render when opened in **OpenOffice.org Writer** version 2.3.0. By upgrading the **OpenOffice.org** suite to 3.1.1-19.5 this issue is no longer presented. ([BZ#527933](#)<sup>1618</sup>)
- the **OpenOffice.org Calc** application would crash when custom colors were created. These updated packages fix an improperly declared variable that caused the bug. Custom colors can now be created successfully. ([BZ#530355](#)<sup>1619</sup>)

As well, these updated packages add the following enhancement:

- the **OpenOffice.org** package prior to version 3.1.1 did not support **Microsoft 2007 Office Open XML** (OOXML) file formats resulting in the inability to open files of this type. The **OpenOffice.org** 3.1.1-19.5 suite provides the necessary support to open OOXML file formats including **pptx**, **xlsx** and **docx**. ([BZ#444052](#)<sup>1620</sup>)

Users of **OpenOffice.org** are advised to upgrade to these updated packages, which resolve these issues and add this enhancement.

## 1.144. openssh

### 1.144.1. RHBA-2009:1668: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1668](#)<sup>1621</sup>

Updated openssh packages that fix a bug are now available.

OpenSSH is OpenBSD's SSH (Secure SHell) protocol implementation. These packages include the core files necessary for both the OpenSSH client and server.

These updated openssh packages fix the following bug:

\* when sshd, the SSH daemon, used multiple SFTP channels simultaneously, each SFTP channel leaked a UNIX socket. This leak could eventually cause sshd to consume large amounts of system resources. This update fixes the leak by ensuring that every SFTP channel closes the UNIX socket, with the result that using SFTP with multiple simultaneous channels does not cause sshd to monopolize system resources. ([BZ#537348](#)<sup>1622</sup>)

All users of openssh are advised to upgrade to these updated packages, which resolve this issue.

### 1.144.2. RHBA-2010:0123: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2010:0123](#)<sup>1623</sup>

Updated openssh packages that resolve an issue are now available.

OpenSSH is OpenBSD's SSH (Secure SHell) protocol implementation. These packages include the core files necessary for both the OpenSSH client and server.

These updated openssh packages fix the following bug:

<sup>1622</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=537348](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=537348)



\* in order to comply with the FIPS 140-2 standard, Security Requirements for Cryptographic Modules, `RAND_cleanup()` function calls were added to places where processes, and their child processes, exited, in both the `ssh` program and the `sshd` service. ([BZ#561420](#)<sup>1624</sup>)

All users of `openssh` are advised to upgrade to these updated packages, which resolve this issue.

### 1.144.3. RHSA-2009:1470: Moderate security update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2009:1470](#)<sup>1625</sup>

Updated `openssh` packages that fix a security issue are now available for Red Hat Enterprise Linux 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

OpenSSH is OpenBSD's SSH (Secure Shell) protocol implementation. These packages include the core files necessary for both the OpenSSH client and server.

A Red Hat specific patch used in the `openssh` packages as shipped in Red Hat Enterprise Linux 5.4 (RHSA-2009:1287) loosened certain ownership requirements for directories used as arguments for the `ChrootDirectory` configuration options. A malicious user that also has or previously had non-`chroot` shell access to a system could possibly use this flaw to escalate their privileges and run commands as any system user. ([CVE-2009-2904](#)<sup>1626</sup>)

All OpenSSH users are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing this update, the OpenSSH server daemon (`sshd`) will be restarted automatically.

### 1.144.4. RHBA-2010:0193: bug fix update

Updated `openssh` packages that fix various bugs and add an enhancement are now available.

OpenSSH is OpenBSD's SSH (Secure Shell) protocol implementation. These packages include the core files necessary for both the OpenSSH client and server.

These packages address the following bugs:

\* When `sshd` used multiple SFTP channels simultaneously, each SFTP channel leaked a unix socket. This socket leak could have eventually caused the `sshd` daemon to monopolize system resources. The bug has been fixed with these updated packages by ensuring that there is no socket leak within a subsystem. ([BZ#530358](#)<sup>1627</sup>)

\* If a zero length SSH2 DSA key existed, the `ssh` init script would hang. This issue has been fixed by allowing the `ssh` init script to automatically overwrite any zero length keys that exist. The `ssh` init script now functions as expected, even if a zero length key exists before execution of the script. ([BZ#531738](#)<sup>1628</sup>)

---

<sup>1624</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=561420](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=561420)

<sup>1626</sup> <https://www.redhat.com/security/data/cve/CVE-2009-2904.html>

<sup>1627</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=530358](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=530358)

<sup>1628</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=531738](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=531738)

As well, these updated packages add the following enhancement:

\* A call to `RAND_cleanup()` has been added to `ssh` and `sshd` to clean the PRNG status when exiting the program. This enhancement also ensures FIPS-140-2 compliance. ([BZ#557164](#)<sup>1629</sup>)

All `openssh` users should upgrade to these updated packages, which resolve these issues.

## 1.145. openssl

### 1.145.1. RHSA-2010:0162: Important security update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2010:0162](#)<sup>1630</sup>

Updated `openssl` packages that fix several security issues are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

OpenSSL is a toolkit that implements the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols, as well as a full-strength, general purpose cryptography library.

It was discovered that OpenSSL did not always check the return value of the `bn_wexpand()` function. An attacker able to trigger a memory allocation failure in that function could cause an application using the OpenSSL library to crash or, possibly, execute arbitrary code. ([CVE-2009-3245](#)<sup>1631</sup>)

A flaw was found in the way the TLS/SSL (Transport Layer Security/Secure Sockets Layer) protocols handled session renegotiation. A man-in-the-middle attacker could use this flaw to prefix arbitrary plain text to a client's session (for example, an HTTPS connection to a website). This could force the server to process an attacker's request as if authenticated using the victim's credentials. This update addresses this flaw by implementing the TLS Renegotiation Indication Extension, as defined in RFC 5746. ([CVE-2009-3555](#)<sup>1632</sup>)

Refer to the following Knowledgebase article for additional details about the [CVE-2009-3555](#)<sup>1633</sup> flaw: <http://kbase.redhat.com/faq/docs/DOC-20491>

A missing return value check flaw was discovered in OpenSSL, that could possibly cause OpenSSL to call a Kerberos library function with invalid arguments, resulting in a NULL pointer dereference crash in the MIT Kerberos library. In certain configurations, a remote attacker could use this flaw to crash a TLS/SSL server using OpenSSL by requesting Kerberos cipher suites during the TLS handshake. ([CVE-2010-0433](#)<sup>1634</sup>)

<sup>1629</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=557164](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=557164)

<sup>1631</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3245.html>

<sup>1632</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3555.html>

<sup>1633</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3555.html>

<sup>1634</sup> <https://www.redhat.com/security/data/cve/CVE-2010-0433.html>



All OpenSSL users should upgrade to these updated packages, which contain backported patches to resolve these issues. For the update to take effect, all services linked to the OpenSSL library must be restarted, or the system rebooted.

### 1.145.2. RHSA-2010:0054: Moderate security update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2010:0054](#)<sup>1635</sup>

Updated openssl packages that fix two security issues are now available for Red Hat Enterprise Linux 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

OpenSSL is a toolkit that implements the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols, as well as a full-strength, general purpose cryptography library.

It was found that the OpenSSL library did not properly re-initialize its internal state in the `SSL_library_init()` function after previous calls to the `CRYPTO_cleanup_all_ex_data()` function, which would cause a memory leak for each subsequent SSL connection. This flaw could cause server applications that call those functions during reload, such as a combination of the Apache HTTP Server, `mod_ssl`, PHP, and `cURL`, to consume all available memory, resulting in a denial of service. ([CVE-2009-4355](#)<sup>1636</sup>)

Dan Kaminsky found that browsers could accept certificates with MD2 hash signatures, even though MD2 is no longer considered a cryptographically strong algorithm. This could make it easier for an attacker to create a malicious certificate that would be treated as trusted by a browser. OpenSSL now disables the use of the MD2 algorithm inside signatures by default. ([CVE-2009-2409](#)<sup>1637</sup>)

All OpenSSL users should upgrade to these updated packages, which contain backported patches to resolve these issues. For the update to take effect, all services linked to the OpenSSL library must be restarted, or the system rebooted.

## 1.146. openswan

### 1.146.1. RHBA-2010:0096: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2010:0096](#)<sup>1638</sup>

---

<sup>1636</sup> <https://www.redhat.com/security/data/cve/CVE-2009-4355.html>

<sup>1637</sup> <https://www.redhat.com/security/data/cve/CVE-2009-2409.html>

Updated openswan packages that fix an issue with NSS passwords being logged at run time are now available.

Openswan is a free implementation of Internet Protocol Security (IPsec) and Internet Key Exchange (IKE) for Linux. IPsec uses strong cryptography to provide both authentication and encryption services. These services allow you to build secure tunnels through untrusted networks. Everything passing through the untrusted net is encrypted by the IPsec gateway machine and decrypted by the gateway at the other end of the tunnel. The resulting tunnel is a virtual private network, or VPN.

These packages contain the daemons and userland tools for setting up openswan. They support the NETKEY/XFRM IPsec stack in the default Linux kernel. The openswan 2.6.x-series also supports IKEv2 as described in RFC 4309.

This update addresses the following issue:

\* when an NSS database is created with a password (either in FIPS or non-FIPS mode), access to a private key (associated with a certificate or a raw public key) requires authentication. At authentication time, openswan passes the database password to NSS. Previously, when this happened, openswan also logged the password to `/var/log/secure`. The password could also be seen by running "ipsec barf". With this update, openswan still passes the database password at authentication time but no longer logs it in any fashion. ([BZ#557688](#)<sup>1639</sup>)

All openswan users are advised to upgrade to these updated packages, which resolve this issue.

## 1.146.2. RHBA-2009:1612: bug fix update



### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1612](#)<sup>1640</sup>

Updated openswan packages that fix an issue and enable Openswan to pass the TAHI test suite for HMAC-SHA1-96 support are now available.

Openswan is a free implementation of Internet Protocol Security (IPsec) and Internet Key Exchange (IKE) for Linux. IPsec uses strong cryptography to provide both authentication and encryption services. These services allow you to build secure tunnels through untrusted networks. Everything passing through the untrusted net is encrypted by the IPsec gateway machine and decrypted by the gateway at the other end of the tunnel. The resulting tunnel is a virtual private network, or VPN.

These packages contain the daemons and userland tools for setting up Openswan. They support the NETKEY/XFRM IPsec stack in the default Linux kernel. The Openswan 2.6.x-series also supports IKEv2 as described in RFC 4309.

The TAHI Project IPv6 Ready Test Suite, Phase 2, includes an IKE version 2 test category. Support for the HMAC-SHA1-96 message digest algorithm is required by this category and, previously, Openswan did not include such support. With this update, HMAC-SHA1-96 supported has been added to the openswan package. ([BZ#533883](#)<sup>1641</sup>)

<sup>1639</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=557688](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=557688)

<sup>1641</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=533883](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=533883)

This update fixes the following issue:

\* the FIPS-140-2 standard requires cryptographic modules to provide methods to "zeroize" (meaning: to overwrite with zeroes) all plain text secret and private cryptographic keys and Critical Security Parameters (CSPs). With this update, Openswan uses methods supplied by the NSS library to perform zeroization on plain text secret and private cryptographic keys and CSPs.

All users of openswan are advised to upgrade to these updated packages, which resolve this issue.

### 1.147. oprofile

#### 1.147.1. RHBA-2010:0283: bug fix and enhancement update

An updated oprofile package that corrects architecture-specific bugs and adds support for Nehalem-EP and IBM POWER7 processors is now available.

OProfile is a system-wide profiler for Linux systems. The profiling runs transparently in the background and profile data can be collected at any time. OProfile uses the hardware performance counters provided on many processors, and can use the Real Time Clock (RTC) for profiling on processors without counters.

This update applies the following fixes and enhancements:

\* An incorrect argument in a binutils library call caused a segmentation fault in oprofile whenever the --debug-info option was used. The elf\_find\_function() function in libbfd required a non-NULL symbol, but oprofile did not receive a warning whenever NULL symbols were present. This update adds an early warning system for this, thereby resulting in more graceful error reporting for the presence of NULL symbols rather than a segmentation fault. ([BZ#450642](https://bugzilla.redhat.com/show_bug.cgi?id=450642)<sup>1642</sup>)

\* OProfile now supports Nehalem-EP processor performance events. ([BZ#498619](https://bugzilla.redhat.com/show_bug.cgi?id=498619)<sup>1643</sup>)

\* When the OProfile daemon started on the Itanium architecture, it created children processes to run perfmon; however, those children processes did not properly close file descriptors for stdin, stdout, and stderr. This could prevent oprofile from properly sending output to any third-party applications. This update corrects the behavior by adding close() functions for open stdin, stdout, and stderr file descriptors, which corrects the daemon behavior on the Itanium architecture. ([BZ#518480](https://bugzilla.redhat.com/show_bug.cgi?id=518480)<sup>1644</sup>)

\* A regression in the binutils-devel static library caused the bfd\_get\_section\_by\_name() function to produce incorrect output. This regression was caused by an error that was present in the binutils-devel specfile when it was compiled. Since OProfile uses binutils-devel at compile time, bfd\_get\_section\_by\_name() also cause oprofile -l to fail. With this release, binutils-devel is compiled with a corrected specfile; OProfile is then re-compiled with this version of binutils-devel, thereby fixing the regression. ([BZ#527679](https://bugzilla.redhat.com/show_bug.cgi?id=527679)<sup>1645</sup>)

\* OProfile now supports the IBM POWER7 processor. ([BZ#566524](https://bugzilla.redhat.com/show_bug.cgi?id=566524)<sup>1646</sup>)

All OProfile users should apply this update.

---

<sup>1642</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=450642](https://bugzilla.redhat.com/show_bug.cgi?id=450642)

<sup>1643</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=498619](https://bugzilla.redhat.com/show_bug.cgi?id=498619)

<sup>1644</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=518480](https://bugzilla.redhat.com/show_bug.cgi?id=518480)

<sup>1645</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=527679](https://bugzilla.redhat.com/show_bug.cgi?id=527679)

<sup>1646</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=566524](https://bugzilla.redhat.com/show_bug.cgi?id=566524)

## 1.148. pam

### 1.148.1. RHBA-2010:0135: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2010:0135](#)<sup>1647</sup>

Updated pam packages that fix a bug in the pam\_time and pam\_group modules are now available.

Pluggable Authentication Modules (PAM) provide a system whereby administrators can set up authentication policies, without having to recompile programs to handle authentication.

These updated packages fix the following bug:

\* the pam\_time and pam\_group modules, which support allowing or rejecting authentication based on time and assigning group names respectively, incorrectly matched user, service, or terminal name substrings even if no wildcard was specified in the configuration. For example, "user" and "user1" were incorrectly equated, causing policies to apply to both usernames even when "user" was the only username subject to said policies. This update improves the string matching in the pam\_time and pam\_group modules ensuring such mis-matches (and consequent policy mis-applications) no longer occur. ([BZ#571341](#)<sup>1648</sup>)

All pam users are advised to upgrade to these updated packages, which resolve this issue.

## 1.149. pam\_krb5

### 1.149.1. RHSA-2010:0258: Low security and bug fix update

Updated pam\_krb5 packages that fix one security issue and various bugs are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having low security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

The pam\_krb5 module allows Pluggable Authentication Modules (PAM) aware applications to use Kerberos to verify user identities by obtaining user credentials at log in time.

A flaw was found in pam\_krb5. In some non-default configurations (specifically, those where pam\_krb5 would be the first module to prompt for a password), the text of the password prompt varied based on whether or not the username provided was a username known to the system. A remote attacker could use this flaw to recognize valid usernames, which would aid a dictionary-based password guess attack. ([CVE-2009-1384](#)<sup>1649</sup>)

This update also fixes the following bugs:

<sup>1648</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=571341](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=571341)

<sup>1649</sup> <https://www.redhat.com/security/data/cve/CVE-2009-1384.html>

\* certain applications which do not properly implement PAM conversations may fail to authenticate users whose passwords have expired and must be changed, or may succeed without forcing the user's password to be changed. This bug is triggered by a previously-applied fix to pam\_krb5 which makes it comply more closely to PAM specifications. If an application misbehaves, enabling the "chpw\_prompt" option for its service should restore the old behavior. ([BZ#509092](#)<sup>1650</sup>)

\* pam\_krb5 does not allow the user to change an expired password in cases where the Key Distribution Center (KDC) is configured to refuse attempts to obtain forwardable password-changing credentials. This update fixes this issue. ([BZ#489015](#)<sup>1651</sup>)

\* failure to verify TGT because of wrong keytab handling. ([BZ#450776](#)<sup>1652</sup>)

Users of pam\_krb5 are advised to upgrade to these updated packages, which resolve these issues.

## 1.150. paps

### 1.150.1. RHBA-2009:1679: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2009:1679](#)<sup>1653</sup>

An updated paps package that fixes a word wrap bug associated with paps' use as the CUPS text filter is now available.

Paps reads UTF-8 encoded text files and renders them to a PostScript file. It uses the pango library to create the outline curves. The paps package also includes the libpaps library, which simplifies PostScript rendering for any pango-based applications (for example, programs that use the GTK+ widget toolkit). As well, paps is used as the CUPS text filter, allowing CUPS to handle UTF-8 encoded strings.

This update addresses the following issue:

\* when paps was used as the CUPS text filter with a "wrap=false" parameter, paps did not honor the parameter: text was wrapped to fit the page despite the parameter instructing otherwise. Paps now calls pango's word wrap functions correctly and, consequently, honors this parameter as expected. ([BZ#520590](#)<sup>1654</sup>)

All paps users should upgrade to this updated package, which resolve this issue.

## 1.151. parted

### 1.151.1. RHBA-2010:0257: bug fix update

Updated parted packages that resolve an issue editing gpt tables are now available.

---

<sup>1650</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=509092](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=509092)

<sup>1651</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=489015](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=489015)

<sup>1652</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=450776](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=450776)

<sup>1654</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=520590](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=520590)

The GNU Parted program allows you to create, destroy, resize, move, and copy hard disk partitions. Parted can be used for creating space for new operating systems, reorganizing disk usage, and copying data to new hard disks.

This update fixes the following problems:

\* when parted is invoked in interactive mode on a disk with GUID Partition Tables (GPT), if the backup GPT is not in the disk's last sector, parted presents an alert;

Error: The backup GPT table is not at the end of the disk, as it should be. This might mean that another operating system believes the disk is smaller. Fix, by moving the backup to the end (and removing the old backup)?

and offers three options for continuing: Fix, Cancel or Ignore. Previously, choosing Cancel or Ignore had no effect: no matter what option was chosen, parted "fixed" (ie changed) the GUID partition table. This update corrects this: if and when the above error presents, the Cancel and Ignore options are now honored if selected, as expected. ([BZ#529672](#)<sup>1655</sup>)

\* When parted is invoked on a disk, it checks to see if there is a file system it recognizes on the partitions on the disk.

When parted was invoked on a dasd disk, and one of the partitions on the disk did not contain a filesystem (such as for example a partition which is a lvm physical volume), then parted would crash due to a NULL pointer dereference. Parted now no longer crashes under these circumstances. ([BZ#563266](#)<sup>1656</sup>)

All parted users should install the updated package, which resolve these issues.

## 1.152. pax

### 1.152.1. RHBA-2009:1591: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2009:1591](#)<sup>1657</sup>

An updated pax package that fixes a bug is now available.

pax is the portable archive exchange utility. It is defined by a POSIX specification, and is able to compress and decompress both tar and cpio archives, as well as several of their older variants.

This updated pax package fixes the following bug:

\* the pax utility creates ustar (Uniform Standard Tape Archive) archives by default. Attempting to create a ustar archive of a directory which contained path names that were exactly 100 characters in length caused pax to fail with the following error message:

<sup>1655</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=529672](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=529672)

<sup>1656</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=563266](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=563266)

pax: File name too long for ustar

With this update, creating ustar archives with pax succeeds regardless of the length of the absolute paths names of the files and directories being archived. ([BZ#239001](#)<sup>1658</sup>)

All users of pax are advised to upgrade to this updated package, which resolves this issue.

## 1.153. pciutils

### 1.153.1. RHBA-2009:1592: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTRACK errata [RHBA-2009:1592](#)<sup>1659</sup>

An updated pciutils package that fixes a bug is now available.

The pciutils package contains various utilities for inspecting and manipulating devices connected to the PCI bus.

This updated pciutils package fixes the following bug:

\* the pciutils use PCILIB, a portable, platform-independent library, to talk to PCI cards. By default PCILIB uses the first available access method but switches can be used to control its behavior. The PCILIB AND ITS OPTIONS section of the lspci man page lists two such switches (-H1 and -H2) that did not work as documented.

The -H1 switch was listed as allowing "direct hardware access via Intel configuration mechanism 1" and the -H2 switch as setting PCILIB to use mechanism 2. In the previous pciutils release, however, using either switch on AMD64 or Intel 64 architectures resulted in an "invalid option -- H" error. (Note: the switches worked as expected on 32-bit x86 architectures).

This error was due to the pciutils package not enabling these switches when compiled for 64-bit architectures. With this update the pciutils spec file includes a corrected build script which enables these features for AMD64 and Intel 64 and, consequently, provides Intel configuration mechanism support to 64-bit architectures as documented. ([BZ#505557](#)<sup>1660</sup>)

All pciutils users should upgrade to this updated package, which resolves this issue.

## 1.154. pcsc-lite

### 1.154.1. RHBA-2010:0278: bug fix update

An updated pcsc-lite package that fixes a bug in the source RPM is now available.

pcsc-lite is a daemon which controls access to smart cards and other security tokens on your system.

---

<sup>1658</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=239001](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=239001)

<sup>1660</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=505557](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=505557)



This update addresses the following issue:

\* the .spec file for the pcsc-lite source rpm contained an error in its Release field. The {dist} tag was not appended to the Release value as a conditional. It was "{dist}" where it should have been "{?dist}". The question mark translates to "If %{dist} is defined, insert its value here. If not, do nothing." Without the question mark, the tag means "dist" is defined and insert its value here. Consequently, if the source rpm was re-built in an environment where the dist variable was not set, the resultant .rpm file contained garbage characters in its file name. This release corrects this. The tag is now a conditional and rebuilding pcse-lite from the source rpm produces an rpm file with the expected file name. ([BZ#440627](#)<sup>1661</sup>)

Only users who use smart cards or security tokens who also rebuild components such as pcsc-lite from source need to update this package.

## 1.155. perl-Sys-Virt

### 1.155.1. RHBA-2010:0251: bug fix update

An updated perl-Sys-Virt package that fixes several bugs is now available.

The Sys::Virt module provides a Perl XS binding to the libvirt virtual machine management APIs. This allows machines running within arbitrary virtualization containers to be managed with a consistent API.

This update addresses the following issues:

\* a number of calls available in the C API, including virStorageVolLookupByKey, virStorageVolLookupByName, and virStorageVolLookupByPath, did not contain Perl bindings. As a result, these storage functions were unavailable when using Perl-based tools for virtual machine management. This update adds the missing calls to the Perl API, and Perl-based management of virtual machines is now possible. ([BZ#519647](#)<sup>1662</sup>)

\* the 'message' subroutine of Error.pm returned an error code instead of an error message. As a consequence, error conditions that required a textual error message instead received an alpha-numeric error code. The 'message' subroutine has been amended to return a textual message, and error conditions now produce a more informative error description. ([BZ#525091](#)<sup>1663</sup>)

\* Sys::Virt did not document the 'flags' parameter used by several methods, including the following:

```
* $vmm->num_of_node_devices * $vmm->list_node_device_names * $vmm->find_storage_pool_sources * $dom->core_dump * $dom->reboot * $dom->block_peek * $dom->memory_peek * $dom->get_autostart * $pool->refresh * $pool->build * $pool->delete
```

Since the 'flags' parameter is currently unused, the parameter and its default value were not mentioned in the methods' descriptions. This could cause certain operations that referenced the 'flags' parameter to fail with a usage error. The 'flags' parameter is now documented as an optional parameter that defaults to a value of zero if it is omitted. Usage errors no longer occur when using the methods as documented. ([BZ#519712](#)<sup>1664</sup>)

<sup>1661</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=440627](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=440627)

<sup>1662</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=519647](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=519647)

<sup>1663</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=525091](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=525091)

<sup>1664</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=519712](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=519712)

\* the description of the `$dom->reboot` method made reference to a list of `&Sys::Virt::Domain::REBOOT_*` constants for use with the 'flags' parameter. However, since the 'flags' parameter is not currently used, the reboot constants were not included in the document. This could cause confusion when implementing the `$dom->reboot` method. The reference to the reboot constants has been removed from the documentation, and the correct usage of the `$dom->reboot` method is now clearer. ([BZ#543878](#)<sup>1665</sup>)

All users using Perl or Perl-based tools to do virtual machine management should install this updated package which fixes these bugs.

## 1.156. perl-XML-SAX

### 1.156.1. RHBA-2010:0008: and perl-XML-LibXML bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2010:0008](#)<sup>1666</sup>

Updated perl-XML-SAX and perl-XML-LibXML packages that fix various bugs are available.

XML::SAX is a SAX parser access API for Perl. It includes classes and APIs required for implementing SAX drivers, along with a factory class for returning any SAX parser installed on the user's system. XML::LibXML provides a library for working with XML files.

These updated perl-XML-SAX and perl-XML-LibXML packages provide the following bug fixes:

\* UTF-8 would not be represented correctly by the perl-XML-SAX parser because the Unicode version of XML::SAX::PurePerl::Reader::switch\_encoding\_string() used Encode::from\_to() that did not set the Perl internal UTF-8 flag. This bug has been corrected by replacing the use of Encode::from\_to() with the use of Encode::decode(). ([BZ#475250](#)<sup>1667</sup>)

\* When upgrading to Red Hat Enterprise Linux 5, a later version or upgrading the individual perl-XML-SAX-0.14 package to perl-XML-SAX-0.14-6, error messages concerning the perl-XML-SAX package would be logged in the `/root/upgrade.log` file. These messages occurred because of a missing file or file data within ParserDetails.ini. This file has been restored to the perl-XML-SAX and perl-XML-LibXML packages with this update. ([BZ#289061](#)<sup>1668</sup>,

[BZ#538855](#)<sup>1669</sup>, [BZ#536819](#)<sup>1670</sup>)

Warning, both perl-XML-SAX and perl-XML-LibXML packages must be updated together in one step. Updating these packages separately can result in the configuration file ParserDetails.ini becoming broken.

All users of perl-XML-SAX and perl-XML-LibXML are advised to upgrade to these updated packages, which resolve these issues.

---

<sup>1665</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=543878](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=543878)

<sup>1667</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=475250](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=475250)

<sup>1668</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=289061](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=289061)

<sup>1669</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=538855](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=538855)

<sup>1670</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=536819](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=536819)

## 1.157. pexpect

### 1.157.1. RHBA-2009:1508: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2009:1508](#)<sup>1671</sup>

An updated pexpect package that fixes two bugs is now available.

pexpect is a pure Python module for spawning child applications, controlling them, and responding to expected patterns in their output. Pexpect works like Don Libes' Expect. Pexpect allows your script to spawn a child application and control it as if a human were typing commands. Pexpect can be used for automating interactive applications such as ssh, ftp, passwd, telnet, etc. It can also be used to automate setup scripts for duplicating software package installations on different servers and for automated software testing.

This update addresses the following issues:

\* pexpect was previously included in the unsupported Extra Packages for Enterprise Linux (EPEL) repository. It is now a supported package in Red Hat Enterprise Linux but is otherwise unchanged. The initial release of pexpect as a supported package included no changes at all and, as a consequence, did not obsolete the EPEL version. To ensure the supported package properly obsoletes the EPEL package, the Release value for this package was incremented. ([BZ#481380](#)<sup>1672</sup>)

\* previously, the shebang lines in pexpect's python executables pointed to "/usr/bin/env python" rather than explicitly referencing the version of Python installed on the system. This broke these executables in the case of a user installing an alternative Python version. With this update, all shebang lines point explicitly to the system version at /usr/bin/python. ([BZ#521891](#)<sup>1673</sup>)

All pexpect users should install this updated package, which addresses these issues.

## 1.158. php

### 1.158.1. RHSA-2010:0040: Moderate security update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2010:0040](#)<sup>1674</sup>

Updated php packages that fix several security issues are now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

<sup>1672</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=481380](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=481380)

<sup>1673</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=521891](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=521891)

PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Web server.

Multiple missing input sanitization flaws were discovered in PHP's exif extension. A specially-crafted image file could cause the PHP interpreter to crash or, possibly, disclose portions of its memory when a PHP script tried to extract Exchangeable image file format (Exif) metadata from the image file. ([CVE-2009-2687](#)<sup>1675</sup>, [CVE-2009-3292](#)<sup>1676</sup>)

A missing input sanitization flaw, leading to a buffer overflow, was discovered in PHP's gd library. A specially-crafted GD image file could cause the PHP interpreter to crash or, possibly, execute arbitrary code when opened. ([CVE-2009-3546](#)<sup>1677</sup>)

It was discovered that PHP did not limit the maximum number of files that can be uploaded in one request. A remote attacker could use this flaw to instigate a denial of service by causing the PHP interpreter to use lots of system resources dealing with requests containing large amounts of files to be uploaded. This vulnerability depends on file uploads being enabled (which it is, in the default PHP configuration). ([CVE-2009-4017](#)<sup>1678</sup>)

Note: This update introduces a new configuration option, `max_file_uploads`, used for limiting the number of files that can be uploaded in one request. By default, the limit is 20 files per request.

It was discovered that PHP was affected by the previously published "null prefix attack", caused by incorrect handling of NUL characters in X.509 certificates. If an attacker is able to get a carefully-crafted certificate signed by a trusted Certificate Authority, the attacker could use the certificate during a man-in-the-middle attack and potentially confuse PHP into accepting it by mistake. ([CVE-2009-3291](#)<sup>1679</sup>)

It was discovered that PHP's `htmlspecialchars()` function did not properly recognize partial multi-byte sequences for some multi-byte encodings, sending them to output without them being escaped. An attacker could use this flaw to perform a cross-site scripting attack. ([CVE-2009-4142](#)<sup>1680</sup>)

All php users should upgrade to these updated packages, which contain backported patches to resolve these issues. After installing the updated packages, the `httpd` daemon must be restarted for the update to take effect.

### 1.158.2. RHBA-2010:0241: bug fix and enhancement update

Updated php packages that fix various bugs and add enhancements are now available.

PHP is an HTML-embedded scripting language that allows developers to write dynamically generated web pages. PHP is ideal for writing database-enabled websites, with built-in integration for several commercial and non-commercial database management systems. PHP is often used as a replacement for CGI scripts.

The php package contains a module that adds support for the PHP language to the Apache HTTP Server.

\* two minor fixes were performed in the php `substr_compare` and `substr_count` functions to correct integer overflows. ([BZ#469807](#)<sup>1681</sup> & [BZ#470971](#)<sup>1682</sup>)

---

<sup>1675</sup> <https://www.redhat.com/security/data/cve/CVE-2009-2687.html>

<sup>1676</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3292.html>

<sup>1677</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3546.html>

<sup>1678</sup> <https://www.redhat.com/security/data/cve/CVE-2009-4017.html>

<sup>1679</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3291.html>

<sup>1680</sup> <https://www.redhat.com/security/data/cve/CVE-2009-4142.html>

<sup>1681</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=469807](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=469807)

<sup>1682</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=470971](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=470971)

- \* if a PHP script uses `odbc_connect` and the `-lodbcpsql` is being used for PostgreSQL, it will either hang forever or cause a segmentation fault. The default behavior was changed, and the hangs and errors no longer occur. ([BZ#483690](#)<sup>1683</sup>)
- \* the default PHP build was not thread-safe, and became unusable with the worker MPM in `httpd`. It was upgraded to be thread-safe and can now be used as expected. ([BZ#484058](#)<sup>1684</sup>)
- \* when an unsupported character set was used, the PHP `mbstring` module would experience a segmentation fault. A patch was added to resolve a double-free problem, and the segfault no longer occurs. ([BZ#486651](#)<sup>1685</sup>)
- \* when rebuilding PHP on IBM PowerPC architecture, the build would fail. A change was made to the PHP specfile, and a rebuild now works as expected. ([BZ#491050](#)<sup>1686</sup>)
- \* the PHP `move_uploaded_file` function was generating inconsistent destination file permissions. The destination file's permissions are now always determined by the active umask and permissions are now consistent. ([BZ#498031](#)<sup>1687</sup>)
- \* some PHP code was creating invalid pointer errors and stack traces. The package was updated so that an entry is added to the log file, and no error occurs. ([BZ#515372](#)<sup>1688</sup>)
- \* the default `memory_limit` value was too low for some 64-bit architectures. The user needed to manually edit the `php.ini` file to be able to start Apache. The default value has been increased to 128M and Apache now starts as expected on 64-bit hardware. ([BZ#517604](#)<sup>1689</sup>)
- \* when attempting to build Zarafa a syntax error caused the build to fail. Extraneous keystrokes were removed and Zarafa now builds as expected. ([BZ#530824](#)<sup>1690</sup>)
- \* the PHP package has been updated to include new code from upstream. ([BZ#500383](#)<sup>1691</sup>, [BZ#505355](#)<sup>1692</sup>, & [BZ#511175](#)<sup>1693</sup>)

Users are advised to upgrade to these updated php packages, which resolve these issues and add these enhancements.

## 1.159. pidgin

### 1.159.1. RHBA-2010:0176: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2010:0176](#)<sup>1694</sup>

<sup>1683</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=483690](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=483690)

<sup>1684</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=484058](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=484058)

<sup>1685</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=486651](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=486651)

<sup>1686</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=491050](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=491050)

<sup>1687</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=498031](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=498031)

<sup>1688</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=515372](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=515372)

<sup>1689</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=517604](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=517604)

<sup>1690</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=530824](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=530824)

<sup>1691</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=500383](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=500383)

<sup>1692</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=505355](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=505355)

<sup>1693</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=511175](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=511175)

Updated pidgin packages that fix a bug are now available.

Pidgin allows you to talk to anyone using a variety of messaging protocols including AIM, MSN, Yahoo!, Jabber, Bonjour, Gadu-Gadu, ICQ, IRC, Novell Groupwise, QQ, Lotus Sametime, SILC, Simple and Zephyr.

These updated pidgin packages fix the following bug:

\* Pidgin users who attempted to log on to an AOL Instant Messenger (AIM) account found that their connections failed due to recent AIM protocol changes. A workaround for this incompatibility involved disabling secure authentication. This update resolves the incompatibility so that Pidgin users are once again able to log on to their AOL Instant Messenger accounts using secure authentication. ([BZ#576311](https://bugzilla.redhat.com/show_bug.cgi?id=576311)<sup>1695</sup>)

All users of pidgin are advised to upgrade to these updated packages, which resolve this issue.

## 1.160. piranha

### 1.160.1. RHBA-2010:0297: bug fix update

Updated piranha packages that fix several bugs are now available.

Piranha provides high-availability and load balancing services for Red Hat Enterprise Linux. It includes various tools to administer and configure the Linux Virtual Server (LVS), as well as the heartbeat and failover components. LVS is a dynamically-adjusted kernel routing mechanism that provides load balancing, primarily for Web and FTP servers.

This update fixes the following bugs:

\* Stopping pulse service does not stop service monitors. In this updated package, pulse will stop all service monitors. ([BZ#522230](https://bugzilla.redhat.com/show_bug.cgi?id=522230)<sup>1696</sup>)

\* Nanny does not work with port different than 80 when monitoring is not provided. In this updated package, nanny works correctly. ([BZ#533113](https://bugzilla.redhat.com/show_bug.cgi?id=533113)<sup>1697</sup>)

\* Nanny does not set port on real server correctly if port on LVS is not 80. In this update package, nanny set port correctly. ([BZ#549738](https://bugzilla.redhat.com/show_bug.cgi?id=549738)<sup>1698</sup>)

\* Pulse does not activate sorry server when all real servers are down. In this updated package, pulse will activate sorry server when needed. ([BZ#566140](https://bugzilla.redhat.com/show_bug.cgi?id=566140)<sup>1699</sup>)

Users of piranha are advised to upgrade to these updated packages, which resolve these issues.

---

<sup>1695</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=576311](https://bugzilla.redhat.com/show_bug.cgi?id=576311)

<sup>1696</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=522230](https://bugzilla.redhat.com/show_bug.cgi?id=522230)

<sup>1697</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=533113](https://bugzilla.redhat.com/show_bug.cgi?id=533113)

<sup>1698</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=549738](https://bugzilla.redhat.com/show_bug.cgi?id=549738)

<sup>1699</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=566140](https://bugzilla.redhat.com/show_bug.cgi?id=566140)

## 1.161. pirut

### 1.161.1. RHBA-2010:0058: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2010:0058](#)<sup>1700</sup>

An updated pirut package that fixes various bugs is now available.

The pirut graphical package manager front end provides a set of graphical tools for managing software.

This updated pirut package includes fixes for the following bugs:

- \* removing a package with pirut when no repositories were configured caused pirut to exit with a Python traceback. With this update, the application does not exit with a traceback when a package is removed in the absence of any configured repositories. ([BZ#444697](#)<sup>1701</sup>)
- \* occasionally, a failed assertion check related to the progress bar, and specifically to the `gtk_progress_set_percentage()` function, caused the pirut package manager to exit with a traceback. This update ensures that this assertion no longer fails, thus resolving the problem. ([BZ#459489](#)<sup>1702</sup>)
- \* after upgrading to the Red Hat Enterprise Linux 5.3 release, pirut began showing the epoch number as the first characters in the package group details list. With this update, package lists are once again sorted correctly. ([BZ#478834](#)<sup>1703</sup>)
- \* the "pup" graphical package manager application used an incorrectly-sized icon. ([BZ#436193](#)<sup>1704</sup>)

All users of pirut are advised to upgrade to this updated package, which resolves these issues.

## 1.162. polycoreutils

### 1.162.1. RHBA-2010:0208: bug fix update

Updated polycoreutils packages that fix several bugs are now available.

The polycoreutils packages contain the core utilities that are required for the basic operation of a Security-Enhanced Linux (SELinux) system and its policies. These utilities include `load_policy` to load policies, `setfiles` to label file systems, `newrole` to switch roles, and `run_init` to run `/etc/init.d/` scripts in their proper context.

These updated packages fix the following bugs:

<sup>1701</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=444697](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=444697)

<sup>1702</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=459489](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=459489)

<sup>1703</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=478834](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=478834)

<sup>1704</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=436193](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=436193)



\* executing the `semanage` command with the translation option caused denials and undesired mode changes to the `setrans.conf` file. This update removes the translation functionality from the `semanage` command. ([BZ#460970](#)<sup>1705</sup>)

\* the `semanage` command allowed an invalid network port number to be passed to it. This update adds proper verification of the port number option to `semanage`. Any invalid port number is now rejected. ([BZ#505521](#)<sup>1706</sup>)

\* the use of the `#!/usr/bin/env python` option at the top of python scripts is being phased out, in favour of the `#!/usr/bin/python` option. There was one instance of the former option in a `polycoreutils` python script. This fix replaces this line with the latter option in this file. ([BZ#521298](#)<sup>1707</sup>)

\* the `semanage` command did not support the `node` option being passed to it and resulted in an error when it was used. This fix adds the `node` option to the `semanage` command. This option allows you to list, add and modify nodes in SELinux policy. ([BZ#527487](#)<sup>1708</sup>)

Users of `polycoreutils` are advised to upgrade to these updated packages, which resolve these issues.

## 1.163. poppler

### 1.163.1. RHSA-2009:1504: Important security and bug fix update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2009:1504](#)<sup>1709</sup>

Updated `poppler` packages that fix multiple security issues and a bug are now available for Red Hat Enterprise Linux 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

`Poppler` is a Portable Document Format (PDF) rendering library, used by applications such as `Evince`.

Multiple integer overflow flaws were found in `poppler`. An attacker could create a malicious PDF file that would cause applications that use `poppler` (such as `Evince`) to crash or, potentially, execute arbitrary code when opened. ([CVE-2009-3603](#)<sup>1710</sup>, [CVE-2009-3608](#)<sup>1711</sup>, [CVE-2009-3609](#)<sup>1712</sup>)

Red Hat would like to thank Chris Rohlf for reporting the [CVE-2009-3608](#)<sup>1713</sup> issue.

---

<sup>1705</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=460970](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=460970)

<sup>1706</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=505521](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=505521)

<sup>1707</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=521298](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=521298)

<sup>1708</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=527487](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=527487)

<sup>1710</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3603.html>

<sup>1711</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3608.html>

<sup>1712</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3609.html>

<sup>1713</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3608.html>

This update also corrects a regression introduced in the previous poppler security update, RHSA-2009:0480, that prevented poppler from rendering certain PDF documents correctly. ([BZ#528147](#)<sup>1714</sup>)

Users are advised to upgrade to these updated packages, which contain backported patches to resolve these issues.

## 1.164. postgresql

### 1.164.1. RHSA-2009:1484: Moderate security update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2009:1484](#)<sup>1715</sup>

Updated postgresql packages that fix two security issues are now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

PostgreSQL is an advanced object-relational database management system (DBMS).

It was discovered that the upstream patch for [CVE-2007-6600](#)<sup>1716</sup> included in the Red Hat Security Advisory RHSA-2008:0038 did not include protection against misuse of the RESET ROLE and RESET SESSION AUTHORIZATION commands. An authenticated user could use this flaw to install malicious code that would later execute with superuser privileges. ([CVE-2009-3230](#)<sup>1717</sup>)

A flaw was found in the way PostgreSQL handled encoding conversion. A remote, authenticated user could trigger an encoding conversion failure, possibly leading to a temporary denial of service. Note: To exploit this issue, a locale and client encoding for which specific messages fail to translate must be selected (the availability of these is determined by an administrator-defined locale setting). ([CVE-2009-0922](#)<sup>1718</sup>)

Note: For Red Hat Enterprise Linux 4, this update upgrades PostgreSQL to version 7.4.26. For Red Hat Enterprise Linux 5, this update upgrades PostgreSQL to version 8.1.18. Refer to the PostgreSQL Release Notes for a list of changes:

<http://www.postgresql.org/docs/7.4/static/release.html> <http://www.postgresql.org/docs/8.1/static/release.html>

All PostgreSQL users should upgrade to these updated packages, which resolve these issues. If the postgresql service is running, it will be automatically restarted after installing this update.

<sup>1714</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=528147](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=528147)

<sup>1716</sup> <https://www.redhat.com/security/data/cve/CVE-2007-6600.html>

<sup>1717</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3230.html>

<sup>1718</sup> <https://www.redhat.com/security/data/cve/CVE-2009-0922.html>

## 1.165. ppc64-utils

### 1.165.1. RHBA-2010:0225: bug fix and enhancement update

Updated ppc64-utils packages that fix various bugs and add various enhancements are now available.

ppc64-utils is a collection of utilities for Linux running on 64-bit PowerPC platforms.

These packages address the following bugs:

\* A bug existed within the ppc64-utils packages that caused a conflict with the powerpc-utils package from IBM. The power-pc-utils package provides dynamic logical partitioning (DLPAR) support, which is a common virtualization feature on the Power PC platform. This conflict forced a user to first remove the ppc61-utils package before installing the power-pc-utils package. To correct this bug, support for the lsslot and drmgr commands has been added to the ppc64-utils packages, ensuring there is no conflict when installing the powerpc-utils package. The lsslot command provides system configuration data to the user and the drmgr command is required to perform DLPAR operations. ([BZ#512373](https://bugzilla.redhat.com/show_bug.cgi?id=512373)<sup>1719</sup>)

\* When attempting to use the Hardware Management Console (HMC) to display the end to end virtual device topology, no data would be shown. The scripts ls-vscsi, ls-veth and ls-vdev have been added for the HMC to use to retrieve Virtual Input and Output (VIO) information that is used to correlate with the output of lsdevinfo to display the end to end virtual device topology. ([BZ#565518](https://bugzilla.redhat.com/show_bug.cgi?id=565518)<sup>172217211720</sup>)

\* Running lsdevinfo on an IBM POWER6 machine with a Virtual Fibre Channel resulted in incorrect errors and an incorrect device name being displayed. These updated packages make sure only necessary error messages are printed and that the correct device name is shown. ([BZ#565518](https://bugzilla.redhat.com/show_bug.cgi?id=565518)<sup>172517241723</sup>)

As well, these updated packages add the following enhancements:

\* CLI and CIM support has been added for end to end virtual device mapping. This additional infrastructure improves the ease of use of virtualization technology by enabling the end to end virtual device view. ([BZ#514813](https://bugzilla.redhat.com/show_bug.cgi?id=514813)<sup>1726</sup>)

\* Support for the -R parameter and the uniquetype field have been added to the HMC. The -R parameter recursively displays the children of the selected device and the uniquetype field is used by the HMC for filtering. ([BZ#565518](https://bugzilla.redhat.com/show_bug.cgi?id=565518)<sup>172917281727</sup>)

Users of ppc64-utils are advised to upgrade to these updated packages, which resolve these issues and add these enhancements.

---

<sup>1719</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=512373](https://bugzilla.redhat.com/show_bug.cgi?id=512373)

<sup>1722</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=565518](https://bugzilla.redhat.com/show_bug.cgi?id=565518)

<sup>1721</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=565518](https://bugzilla.redhat.com/show_bug.cgi?id=565518)

<sup>1720</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=565518](https://bugzilla.redhat.com/show_bug.cgi?id=565518)

<sup>1725</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=565518](https://bugzilla.redhat.com/show_bug.cgi?id=565518)

<sup>1724</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=565518](https://bugzilla.redhat.com/show_bug.cgi?id=565518)

<sup>1723</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=565518](https://bugzilla.redhat.com/show_bug.cgi?id=565518)

<sup>1726</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=514813](https://bugzilla.redhat.com/show_bug.cgi?id=514813)

<sup>1729</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=565518](https://bugzilla.redhat.com/show_bug.cgi?id=565518)

<sup>1728</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=565518](https://bugzilla.redhat.com/show_bug.cgi?id=565518)

<sup>1727</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=565518](https://bugzilla.redhat.com/show_bug.cgi?id=565518)

## 1.166. procps

### 1.166.1. RHBA-2010:0200: bug fix and enhancement update

An updated procps package that fixes various bugs is now available.

The procps package contains a set of system utilities that provide system information. Procps includes ps, free, skill, pkill, pgrep, snice, tload, top, uptime, vmstat, w, watch and pdwx.

This updated procps package includes fixes for the following bugs:

- \* There was an array in proc/devname.c that was trying to hold bytes in excessive of its capacity, leading to string overflow errors and making the names unusable. A patch has been incorporated that widens the strings so that they include the NUL terminator so that this error no longer occurs. ([BZ#469495](#)<sup>1730</sup>)
- \* The ps command defines a fixed width for user names. If a name exceeds this width, the command will revert to displaying the numeric id instead. This behavior was not properly documented in the man page for the command so it has now been added to make users more clearly aware of this behavior. ([BZ#471476](#)<sup>1731</sup>)
- \* There was an issue when using the slabtop command with the "-o" option. The command's output would immediately disappear instead of being printed to stdout meaning that the information could not be read. slabtop has now been altered so that output is directed to stdout. As a result, users can now read the output on the terminal screen. ([BZ#475963](#)<sup>1732</sup>)
- \* With increases in memory sizes, tools such as vmstat were misaligning the header columns and output for statistics such as free, buff and cache memory. To fix this issue, the "-w" switch has been modified to account for longer figures pertaining to memory statistics. With these wider fields, the columns and their headers are now correctly aligned. ([BZ#484789](#)<sup>1733</sup>)
- \* The ps command would occasionally throw a double-free corruption error. This would cause the software to die unexpectedly. This has been fixed by adding a test that looks for zero at the end of a process. As a result, ps no longer aborts unexpectedly. ([BZ#487700](#)<sup>1734</sup>)
- \* The "sysctl -a" command was using deprecated syscalls. The software has been modified so that it no longer uses these deprecated calls. As a result, when the archaic code is eventually removed, sysctl will continue to work. A warning message has also been removed from the package's man page. ([BZ#501785](#)<sup>1735</sup> [BZ#556508](#)<sup>1736</sup>)
- \* The ps command was not producing a core dump when it crashed, making it extremely hard to troubleshoot. Code to handle SIGABRT and SIGSEGV has now been added to the software so that it will produce a core dump if it crashes. As a result, problems will be much easier to trace. ([BZ#512857](#)<sup>1737</sup>)
- \* The ps utility's "etime" field shows the elapsed time since a process was started. On heavily-loaded systems, it was possible for a negative value to be returned due to an integer overflow. This has been

---

<sup>1730</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=469495](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=469495)

<sup>1731</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=471476](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=471476)

<sup>1732</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=475963](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=475963)

<sup>1733</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=484789](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=484789)

<sup>1734</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=487700](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=487700)

<sup>1735</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=501785](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=501785)

<sup>1736</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=556508](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=556508)

<sup>1737</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=512857](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=512857)

rectified so that it always correctly returns a positive value, thus providing users with accurate data.. ([BZ#556762](#)<sup>1738</sup>)

\* If the user pressed "f" whilst running top and selected a low number of fields, erroneous and jumbled text would appear at the top of the screen. The top utility has now been modified so that the text clears correctly and the output is displayed as one would expect. ([BZ#556777](#)<sup>1739</sup>)

\* The vmstat utility has a field entitled "Time stolen from a virtual machine." Unfortunately, the addition of the "-w" switch had an adverse impact upon the way this information was output. Consequentially, when vmstat was run in default mode, the field's header was missing and when it was run with the "-w" option, it disappeared altogether. A patch has now been added and, as a result, the field now displays correctly at all times. ([BZ#558475](#)<sup>1740</sup>)

\* The "pmap -x" command was not displaying the resident set size (RSS) for process ids. No figures were appearing in the column. A patch has been applied so that the figures for this field are now correctly calculated and displayed. ([BZ#561392](#)<sup>1741</sup>)

Users are advised to upgrade to this updated procps package, which resolves these issues.

## 1.167. pykickstart

### 1.167.1. RHBA-2010:0248: bug fix and enhancement update

An updated pykickstart package that fixes two bugs and adds three enhancements is now available.

The pykickstart package is a python library used to manipulate kickstart files.

This updated package fixes the following bugs:

\* The anaconda installation system would crash when attempting to write guest installation files to a iscsi connected host. This was because pykickstart did not specify an iscsi port for use in the installation. This behaviour has been corrected and pykickstart now specifies a default iscsi port. ([BZ#547678](#)<sup>1742</sup>)

\* The update which enabled the --hvargs boot option in pykickstart (see [BZ#547877](#)<sup>1744</sup><sup>1743</sup>) caused anaconda to return the error: "KeyError: 'hvArgs'" and exit the installation. A patch has been applied to kickstart.py to correct this. ([BZ#540473](#)<sup>1745</sup>)

This update also adds the following enhancements:

\* pykickstart now has an additional bootloader option (--hvargs) which allows kernel arguments for the hypervisor to be specified in the kickstart file. ([BZ#547877](#)<sup>1747</sup><sup>1746</sup>)

\* pykickstart now adds the kickstart line number of a script to anaconda error logs if that script causes the installation to fail. This assists with debugging kickstart installation problems. ([BZ#547188](#)<sup>1748</sup>)

---

<sup>1738</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=556762](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=556762)

<sup>1739</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=556777](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=556777)

<sup>1740</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=558475](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=558475)

<sup>1741</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=561392](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=561392)

<sup>1742</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=547678](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=547678)

<sup>1744</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=547877](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=547877)

<sup>1743</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=547877](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=547877)

<sup>1745</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=540473](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=540473)

<sup>1747</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=547877](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=547877)

<sup>1746</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=547877](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=547877)

<sup>1748</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=547188](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=547188)

\* The kickstart install process is able to use package group entries to automatically install all packages in a specified 'group'. Functionality has now been added to both pykickstart and the anaconda install system to also support group exclusions, such as `-@conflicts`. ([BZ#555311](#)<sup>1749</sup>).

pykickstart users should upgrade to this updated package, which fixes these issue and adds these enhancements.

## 1.168. python-virtinst

### 1.168.1. RHBA-2010:0282: bug fix and enhancement update

An updated python-virtinst package that fixes bugs and adds enhancements is now available.

python-virtinst is a module that helps build and install libvirt based virtual machines.

This updated package addresses the following issues:

\* When installing a KVM Windows guest with virt-install, QEMU would not immediately recognise the installation. An error message would appear, despite a successful installation. A minor delay has been added to allow the correct information to be gathered, and the incorrect error message no longer appears. ([BZ#498237](#)<sup>1750</sup>)

\* An unsupported `--prompt` option was listed in the `--help` output for virt-image. When virt-image `--prompt` was run, an error message would print. The `--prompt` option has been removed from the `--help` output. ([BZ#503721](#)<sup>1751</sup>)

\* cow, qcow and qcow2 were not listed in the virt-convert format whitelist, although they were supported. An unknown disk format error would print for each format when virt-convert was run from a VMware virtual machine to a virt-image. cow, qcow and qcow2 are now listed.

([BZ#506927](#)<sup>1752</sup>)

\* virt-install would fail when re-installing a virtual system using an .img file that had been moved or deleted, instead of re-creating the guest image. The error was found to be spurious characters in the image paths ('/'). Code has been corrected in python-virtinst to prevent this error. ([BZ#511925](#)<sup>1753</sup>)

\* By default, virtual disks are not opened with `O_DIRECT`. This meant data would sometimes be cached twice: once inside the virtual machine, and once outside. Users had to manually add `<driver name='qemu' cache='none'/>` to the virtual machine definition to prevent double caching. The default cache mode of QEMU and KVM guests is now set to "none", which prevents inconsistent disc states. ([BZ#512072](#)<sup>1754</sup>)

\* The `--disk` option of virt-install was not compatible with the `--prompt` option, and caused error messages to print when they were used together. The interaction between these two options has been adjusted, and `--disk` can now be used with `--prompt` successfully. ([BZ#516129](#)<sup>1755</sup>)

\* When `--wait` is specified as 0, virt-install should begin the installation process and exit the console. However, a syntax error in the code caused virt-install `--wait` to perform as if it was not specified, and

<sup>1749</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=555311](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=555311)

<sup>1750</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=498237](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=498237)

<sup>1751</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=503721](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=503721)

<sup>1752</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=506927](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=506927)

<sup>1753</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=511925](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=511925)

<sup>1754</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=512072](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=512072)

<sup>1755</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=516129](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=516129)

the console must be closed manually. The syntax error has now been corrected, and if `--wait=0`, the installation process will begin and close the console. (BZ#517081<sup>1756</sup>)

\* When running `virt-install --prompt --nographics`, if the disk size was too big for the available disk space, a badly formatted error message would print. The error message syntax has been corrected, and the user prompt now appears on a new line beneath the message. (BZ#523767<sup>1757</sup>)

\* `virt-install` reported that the installation was still in progress after the installation was complete and the guest machine was being rebooted. The post installation error catching and reporting has been improved. The guest state is now reported accurately. (BZ#545837<sup>1758</sup>)

\* An `os` dictionary entry has been backported into this release. Users no longer need to use `virtio26` to enable `virtio` support for guests. This entry can be selected in `virt-manager` or via `virt-install --os-variant`. (BZ#547380<sup>1759</sup>)

\* `libvirt` was, at times, unable to start guest systems when installing under a minor load, and the install would fail. There were memory problems if another process was writing to disk simultaneously, and `virt-install` was misreading nonsparse disk images. This fix modifies the `libvirt` timeout manager to better cope with shared I/O conditions and adds the `O_DSYNC` flag to `python-virtinst` to manage nonsparse disk reading. (BZ#558855<sup>1760</sup>)

\* Previously, a patch was added to `virtinst` to avoid non-sparse volume creation, because `libvirt` did not drop the pool lock while allocating. However, the `libvirt` version in this release does not have this issue. The patch has been removed and `virt-install` no longer ignores `--nonsparse` when creating an image inside `libvirt`'s storage pool. (BZ#569339<sup>1761</sup>)

Users are advised to upgrade to this updated `python-virtinst` package which resolves these issues.

## 1.169. PyXML

### 1.169.1. RHSA-2010:0002: Moderate security update



#### Important

This update has already been released (prior to the GA of this release) as the security errata *RHSA-2010:0002*<sup>1762</sup>

An updated `PyXML` package that fixes one security issue is now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

`PyXML` provides XML libraries for Python. The distribution contains a validating XML parser, an implementation of the SAX and DOM programming interfaces, and an interface to the Expat parser.

---

<sup>1756</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=517081](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=517081)

<sup>1757</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=523767](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=523767)

<sup>1758</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=545837](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=545837)

<sup>1759</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=547380](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=547380)

<sup>1760</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=558855](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=558855)

<sup>1761</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=569339](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=569339)



A buffer over-read flaw was found in the way PyXML's Expat parser handled malformed UTF-8 sequences when processing XML files. A specially-crafted XML file could cause Python applications using PyXML's Expat parser to crash while parsing the file. ([CVE-2009-3720](#)<sup>1763</sup>)

This update makes PyXML use the system Expat library rather than its own internal copy; therefore, users must install the RHTSA-2009:1625 expat update together with this PyXML update to resolve the [CVE-2009-3720](#)<sup>1764</sup> issue.

All PyXML users should upgrade to this updated package, which changes PyXML to use the system Expat library. After installing this update along with RHTSA-2009:1625, applications using the PyXML library must be restarted for the update to take effect.

## 1.170. qspice

### 1.170.1. RHBA-2009:1489: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1489](#)<sup>1765</sup>

Updated qspice packages that fix several bugs are now available.

The Simple Protocol for Independent Computing Environments (SPICE) is a remote display protocol designed for virtual environments. SPICE users can view a virtualized desktop or server from the local system or any system with network access to the server. SPICE is available for a variety of machine architectures and operating systems. SPICE is used in Red Hat Enterprise Linux for viewing virtualized guests running on the KVM hypervisor or on Red Hat Enterprise Virtualization Hypervisors.

These updated packages fix the following bugs:

\* the SPICE server uses a heuristic method for detecting video streams. Some sites, however, send two video frame pixmaps: the actual size of the frame and a variant that measures from the top-left of the web-page presenting the frame to the bottom-right of the video frame. Receiving two video pixmaps caused the SPICE heuristic to fail to detect the video stream. This failure also caused a dramatic increase in CPU use and network traffic. With this update, the heuristic detects dual-pixmap video streams accurately; video playback occurs as expected and CPU use and network traffic no longer spike. ([BZ#521791](#)<sup>1766</sup>)

\* previously the SPICE server used a fixed bit-rate for video streams. If external factors affected the data stream, this fixed bit-rate resulted in dropped frames and low quality playback. With this update, the SPICE server no longer uses a hard-coded bit-rate; instead it can choose a bit-rate that reflects current network conditions, improving video playback in low-bandwidth conditions. ([BZ#521792](#)<sup>1767</sup>)

\* on new client connections the SPICE server previously sent the client an uncompressed initial screen image. In low bandwidth conditions this resulted in a long period of apparent inactivity, with

<sup>1763</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3720.html>

<sup>1764</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3720.html>

<sup>1766</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=521791](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=521791)

<sup>1767</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=521792](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=521792)

the client presenting an unusable black screen. The SPICE server now compresses the initial screen image, greatly reducing initialization time. (BZ#522049<sup>1768</sup>)

Users requiring remote display capabilities for KVM hypervisors are advised to upgrade to these updated qspice packages, which resolve these issues.

### 1.170.2. RHBA-2010:0264: bug fix update

Updated qspice packages that fix various bugs are now available.

The Simple Protocol for Independent Computing Environments (SPICE), a remote display protocol used in Red Hat Enterprise Linux for viewing virtualized guests running on the KVM hypervisor or on Red Hat Enterprise Virtualization Hypervisors.

The updated packages fix the following bugs:

\* previously, if some sites sent two video frame pixmaps, the SPICE heuristic failed to detect the video stream and caused a dramatic increase in CPU use and network traffic. With this update, the dual-pixmap video streams is detected, video playback occurs as expected and CPU use and network traffic no longer spike. (BZ#518193<sup>1769</sup>)

\* the SPICE server previously used a fixed bit-rate for video streams. If external factors affected the data stream, this resulted in dropped frames and low quality playback. With this update, the SPICE server no longer uses a hard-coded bit-rate; instead it can choose a bit-rate that reflects current network conditions, improving video playback in low-bandwidth conditions. (BZ#518388<sup>1770</sup>)

\* the SPICE server previously sent a new client connections an uncompressed initial screen image. In low bandwidth conditions this resulted in a long period of apparent inactivity, with the client presenting an unusable black screen. The SPICE server now compresses the initial screen image, greatly reducing initialization time. (BZ#521488<sup>1771</sup>)

\* if configured with SSL, previously a SPICE client would open SSL with DEFLATE compression and the server would accept the compression, resulting in a poor display. Currently, if the client offers SSL compression, the compression is not accepted by the server. (BZ#482111<sup>1772</sup>)

\* the video compression algorithm can start when the guest is accessing text instead of video causing the text to be blurry. The SPICE server now has an improved heuristic for distinguishing between videos and textual streams. (BZ#493375<sup>1773</sup>)

\* VM run on loaded host crashed when SPICE session opened from RHEV Manager Local-Host [trap divide error 0]. (BZ#525055<sup>1774</sup>)

\* sometimes a client was timed out if the server was overloaded or due to low bandwidth. Client timeout has been increased to 15 seconds to prevent this. (BZ#526458<sup>1775</sup>)

\* qemu crashed when OpenOffice 3.1.1 launched .odp files. (BZ#545862<sup>1776</sup>)

---

<sup>1768</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=522049](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=522049)

<sup>1769</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=518193](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=518193)

<sup>1770</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=518388](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=518388)

<sup>1771</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=521488](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=521488)

<sup>1772</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=482111](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=482111)

<sup>1773</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=493375](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=493375)

<sup>1774</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=525055](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=525055)

<sup>1775</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=526458](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=526458)

<sup>1776</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=545862](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=545862)

\* qspice provides an implementation of the qspice server, not the client (which is provided by the spice-client package). Previous qspice builds, however, included spice-client directories and files. These unnecessary files and directories were removed from the qspice package for this update. ([BZ#549532](#)<sup>1777</sup>)

\* destination server authentication during migration process is now supported. The SPICE server sends destination server identity to the client which uses it to authenticate the server. ([BZ#549673](#)<sup>1778</sup>)

\* previous qemu and SPICE server crashes were caused by wrong access to ring items in the code. These have since been resolved. ([BZ#551580](#)<sup>1779</sup> and [BZ#559207](#)<sup>1780</sup>)

\* a video streaming issue caused display of an unclear Welcome button on log-out on a Windows 7 guest. A lower limit to streamable images prevents streaming of images that are probably textual. ([BZ#558270](#)<sup>1781</sup>)

\* in Windows media player 12 full screen mode small videos are scaled directly and sent to the client. SPICE server identified the scaled images as "artificial" and did not stream them. A more permissive heuristic now enables these to be streamed. ([BZ#562744](#)<sup>1782</sup>)

Users requiring remote display capabilities for KVM hypervisors are advised to upgrade to these updated qspice packages which resolve the above issues.

## 1.171. readahead

### 1.171.1. RHBA-2010:0005: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2010:0005](#)<sup>1783</sup>

An updated readahead package that fixes a bug is now available.

readahead reads the contents of a list of files into memory, which causes them to be read from cache when they are actually needed. Its goal is to speed up the boot process.

This update addresses the following bug:

\* readahead includes a python helper script for readahead list maintainers: `/usr/share/doc/readahead-1.3/readahead-check`. Previously, this script's shebang line pointed to `"/usr/bin/env python"` rather than explicitly referencing the Python version installed on the system. This reference broke scripts such as `readahead-check` in the case of a user installing an alternative Python version. With this update, the shebang line in `readahead-check` points explicitly to the system version at `/usr/bin/python`. ([BZ#521280](#)<sup>1784</sup>)

<sup>1777</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=549532](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=549532)

<sup>1778</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=549673](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=549673)

<sup>1779</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=551580](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=551580)

<sup>1780</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=559207](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=559207)

<sup>1781</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=558270](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=558270)

<sup>1782</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=562744](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=562744)

<sup>1784</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=521280](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=521280)

All readahead users should install this update which addresses this issue.

### 1.172. redhat-artwork

#### 1.172.1. RHBA-2010:0311: bug fix update

Updated redhat-artwork packages that remove unnecessary duplicate images are now available.

redhat-artwork contains artwork for the default look and feel of Red Hat Enterprise Linux.

This update addresses the following issues:

\* in the previous release, the directory used to store images for use by the KDE Display Manager -- /usr/share/apps/kdm/themes/RHEL/ -- contained images also present in the directory used by the GNOME Display Manager -- /usr/share/gdm/themes/RHEL/ (GNOME is the default desktop environment for Red Hat Enterprise Linux). For this release, these duplicates were removed and replaced with symlinks to the images in /usr/share/gdm/themes/RHEL/. This reduces the redhat-artwork package's size slightly with no effect on functionality. ([BZ#485978](#)<sup>17861785</sup>)

\* as well, /usr/share/apps/kdm/themes/RHEL/ also contained Red Hat trademarked images that are (and should only be) included in the redhat-logos package. For this update, these trademarked images were removed from redhat-artwork. When a Red Hat trademarked image is displayed, such images are always assumed to be in directories below /usr/share/ other than /usr/share/apps/, so this removal also has no effect on functionality. ([BZ#485978](#)<sup>17881787</sup>)

Users should upgrade to this updated package, which resolves these issues.

### 1.173. redhat-release

#### 1.173.1. RHEA-2010:0207: enhancement update

A new redhat-release package is now available for Red Hat Enterprise Linux 5.5.

The redhat-release package contains licensing information regarding, and identifies the installed version of, Red Hat Enterprise Linux.

This new package reflects changes made for the release of Red Hat Enterprise Linux 5.5.

Users of Red Hat Enterprise Linux 5 should upgrade to this updated package.

### 1.174. redhat-release-notes

#### 1.174.1. RHEA-2010:0315: enhancement update

An updated redhat-release-notes package is now available.

---

<sup>1786</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=485978](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=485978)

<sup>1785</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=485978](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=485978)

<sup>1788</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=485978](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=485978)

<sup>1787</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=485978](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=485978)

An updated version of the redhat-release-notes package is now available as part of ongoing support and maintenance of Red Hat Enterprise Linux 5.

This package contains the release notes for Red Hat Enterprise Linux 5.5.

## 1.175. rgmanager

### 1.175.1. RHBA-2009:1510: bug-fix update



#### Note

This update has already been released (prior to the GA of this release) as errata *RHBA-2009:1510*<sup>1789</sup>

Updated rgmanager packages that fix a bug are available.

The rgmanager packages contain the Red Hat Resource Group Manager, which provides the ability to create and manage high-availability server applications in the event of system downtime.

This update applies the following bug fix:

\* An issue preventing correct handling of Xen virtual machines utilizing the "path" attribute in cluster.conf has been fixed.

Red Hat Resource Group Manager users are advised to upgrade to these updated packages, which address this issue.

### 1.175.2. RHBA-2009:1521: bug-fix update



#### Note

This update has already been released (prior to the GA of this release) as errata *RHBA-2009:1521*<sup>1790</sup>

Updated rgmanager packages that fix two bugs are available.

The rgmanager packages contain the Red Hat Resource Group Manager, which provides the ability to create and manage high-availability server applications in the event of system downtime.

This update applies the following bug fixes:

\* An issue preventing correct handling of bonded links on virtual network bridges when using VLANs has been fixed.

\* An issue preventing killing all processes holding references on a mount point during a force unmount operation has been fixed.

Red Hat Resource Group Manager users are advised to upgrade to these updated packages, which address these issues.

### 1.175.3. RHBA-2009:1589: bug-fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1589](#)<sup>1791</sup>

Updated rgmanager packages that fix a bug are available.

The rgmanager packages contain the Red Hat Resource Group Manager, which provides the ability to create and manage high-availability server applications in the event of system downtime.

This update applies the following bug fix:

\* An issue causing services to get stuck in the 'recovering' state during a failed relocation attempt has been fixed. ([BZ#531799](#)<sup>1792</sup>)

Red Hat Resource Group Manager users are advised to upgrade to these updated packages, which address this issue.

### 1.175.4. RHBA-2010:0280: bug fix and enhancement update

Updated rgmanager packages that fix numerous bugs and add several enhancements are now available.

The rgmanager packages contain the Red Hat Resource Group Manager, which provides the ability to create and manage high-availability server applications in the event of system downtime.

This update addresses the following bugs:

\* failed virtual machine migrations are handled more correctly. ([BZ#499835](#)<sup>1793</sup>)

\* clustered file systems are no longer unmounted after a configuration change. ([BZ#506094](#)<sup>1794</sup>)

\* clustat's output is now consistent when given bad input. ([BZ#506346](#)<sup>1795</sup>)

\* the force\_unmount flag now works correctly when used with HA-LVM. ([BZ#514040](#)<sup>1796</sup>)

\* path support for Xen virtual machines works again. ([BZ#519786](#)<sup>1797</sup>)

\* S/Lang processor no longer leaks memory. ([BZ#507431](#)<sup>1798</sup>)

\* rgmanager exits if killed while waiting for fencing. ([BZ#508147](#)<sup>1799</sup>)

\* bonded link handling when using Xen bridged interfaces works. ([BZ#518037](#)<sup>1800</sup>)

---

<sup>1792</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=531799](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=531799)

<sup>1793</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=499835](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=499835)

<sup>1794</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=506094](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=506094)

<sup>1795</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=506346](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=506346)

<sup>1796</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=514040](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=514040)

<sup>1797</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=519786](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=519786)

<sup>1798</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=507431](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=507431)

<sup>1799</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=508147](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=508147)

<sup>1800</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=518037](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=518037)

- \* services no longer get stuck in the 'recovering' state. ([BZ#530409](#)<sup>1801</sup>)
- \* node rejoins prior to fencing completion are now handled correctly. ([BZ#527777](#)<sup>1802</sup>)
- \* live migration of frozen VMs is an invalid operation. ([BZ#510017](#)<sup>1803</sup>)
- \* tomcast-5.sh now uses su instead of sudo. ([BZ#524757](#)<sup>1804</sup>)
- \* multiple event handlers no longer cause problems with central\_processing. ([BZ#527239](#)<sup>1805</sup>)
- \* ip.sh honors monitor\_link during service start. ([BZ#532756](#)<sup>1806</sup>)
- \* ip.sh now attempts to detect IP address collisions. ([BZ#526647](#)<sup>1807</sup>)
- \* ip.sh now handles ipv6 addresses with shortened quads correctly. ([BZ#533461](#)<sup>1808</sup>)
- \* SAPInstance and SAPDatabase may now be referenced from the <resources/> block. ([BZ#529052](#)<sup>1809</sup>)
- \* fs.sh no longer warns about bind mounts. ([BZ#526286](#)<sup>1810</sup>)
- \* migrating a virtual machine to an offline node returns an error. ([BZ#536157](#)<sup>1811</sup>)
- \* aggressive timeouts causing services to sometimes erroneously enter the 'failed' state have been changed to scale with the cluster's timeout. ([BZ#548133](#)<sup>1812</sup>)
- \* clusvcadm now checks the return code msg\_send. ([BZ#529929](#)<sup>1813</sup>)
- \* 'Depend' attributes when using central processing are handled correctly. ([BZ#523999](#)<sup>1814</sup>)
- \* a bug in HA-LVM which could cause metadata corruption in some cases has been fixed. ([BZ#557167](#)<sup>1815</sup>)

This update also includes the following enhancements:

- \* more debugging information has been added to /tmp/rgmanager-dump.. ([BZ#512052](#)<sup>1816</sup>)
- \* path support emulation has been added for KVM virtual machines. ([BZ#545916](#)<sup>1817</sup>)
- \* vm.sh now provides more meaningful error reports. ([BZ#529926](#)<sup>1818</sup>)

---

<sup>1801</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=530409](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=530409)

<sup>1802</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=527777](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=527777)

<sup>1803</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=510017](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=510017)

<sup>1804</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=524757](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=524757)

<sup>1805</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=527239](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=527239)

<sup>1806</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=532756](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=532756)

<sup>1807</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=526647](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=526647)

<sup>1808</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=533461](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=533461)

<sup>1809</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=529052](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=529052)

<sup>1810</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=526286](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=526286)

<sup>1811</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=536157](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=536157)

<sup>1812</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=548133](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=548133)

<sup>1813</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=529929](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=529929)

<sup>1814</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=523999](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=523999)

<sup>1815</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=557167](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=557167)

<sup>1816</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=512052](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=512052)

<sup>1817</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=545916](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=545916)

<sup>1818</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=529926](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=529926)



\* file system resources now report errors when status checks fail. ([BZ#562237](#)<sup>1819</sup>)

Red Hat Resource Group Manager users are advised to upgrade to these updated packages, which address these issues.

### 1.176. rhn-client-tools

#### 1.176.1. RHBA-2010:0270: bug fix and enhancement update

Updated rhn-client-tools packages that fix several bugs and add enhancements are now available.

Red Hat Network Client Tools provide programs and libraries that allow your system to receive software updates from Red Hat Network (RHN).

This update fixes several bugs and implements new features:

\* support for subscribing to a RHN and RHN Satellite channels using a command line tool. ([BZ#216808](#)<sup>1820</sup>)

\* fix for a problem where a package profile uploaded to RHN or RHN Satellite during system registration was incomplete. (BZ #489901,

[BZ#509265](#)<sup>1821</sup>, [BZ#510798](#)<sup>1822</sup>, [BZ#514625](#)<sup>1823</sup>)

\* require recent version of hal to be able to properly retrieve all dmi related information during system registration. ([BZ#494679](#)<sup>1824</sup>)

\* fix for a problem where dbus and hal services were not running at the end of new system provisioning making it impossible for system registration to RHN or RHN Satellite. Without these services running, registration code was unable to correctly detect a virtualization guest, resulting in the provisioned virtualized system consuming a physical system entitlement. The fix for the problem contains a new method of detecting a virtualization guest when dbus and hal services are not running. ([BZ#495680](#)<sup>1825</sup>)

\* do not limit the output from rhnreg\_ks utility only to a console. This makes it possible for redirection of the output from rhnreg\_ks to a file or a pipe. ([BZ#503146](#)<sup>1826</sup>)

\* fix typo error in up2date manual page. ([BZ#510014](#)<sup>1827</sup>)

\* in network setups where the system is getting a hostname from a DHCP server even though its hostname does not have a valid DNS record, register the system with its hostname. ([BZ#511273](#)<sup>1828</sup>)

\* when registering system to RHN or RHN Satellite using firstboot interface, correctly populate configuration values in /etc/sysconfig/rhn/up2date. ([BZ#513660](#)<sup>1829</sup>)

---

<sup>1819</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=562237](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=562237)

<sup>1820</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=216808](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=216808)

<sup>1821</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=509265](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=509265)

<sup>1822</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=510798](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=510798)

<sup>1823</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=514625](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=514625)

<sup>1824</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=494679](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=494679)

<sup>1825</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=495680](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=495680)

<sup>1826</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=503146](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=503146)

<sup>1827</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=510014](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=510014)

<sup>1828</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=511273](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=511273)

<sup>1829</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=513660](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=513660)

- \* remove unnecessary text window displayed during registration of system. ([BZ#516207](#)<sup>1830</sup>)
- \* when registering a system using network bonding setup, report real hardware addresses of all network interfaces involved in a network bond. ([BZ#517945](#)<sup>1831</sup>)
- \* fix headers of python executable files to comply with Fedora packaging guidelines. ([BZ#521281](#)<sup>1832</sup>)
- \* revised logic of the networkRetries configuration option. Setting the option to '0' will have the same effect as setting to '1'. ([BZ#526450](#)<sup>1833</sup>)
- \* support for package installation date displayed in RHN Satellite web user interface. This feature also requires server-side support. ([BZ#530369](#)<sup>1834</sup>)
- \* fixed traceback occurring during GUI based system registration executed from firstboot environment. ([BZ#530659](#)<sup>1835</sup>)
- \* include the new Red Hat Network Certificate Authority file ([BZ#566479](#)<sup>1836</sup>)

All users of rhn-client-tools are advised to upgrade to these updated packages, which resolve these issues.

## 1.177. rhnlb

### 1.177.1. RHBA-2010:0322: bug fix update

An updated rhnlb package that provides bug fixes and enhancements is now available.

rhnlb is a collection of Python modules used by the Red Hat Network (RHN) software.

This updated package addresses the following bugs:

- \* When attempting to download multiple packages during satellite-sync, the download will fail after the first redirect to the content provider. ([BZ#564299](#)<sup>1837</sup>)

This update also provides the following enhancement:

- \* rhnlb was rebased to version 2.5.22, the latest stable release in the Spacewalk branch. This rebase includes performance improvements and contains an enhancement required in a forthcoming release of RHN Satellite. ([BZ#566694](#)<sup>1838</sup>)

All Red Hat Network Satellite users are advised to upgrade to this updated package, which provides these enhancements and bug fixes.

---

<sup>1830</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=516207](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=516207)

<sup>1831</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=517945](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=517945)

<sup>1832</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=521281](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=521281)

<sup>1833</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=526450](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=526450)

<sup>1834</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=530369](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=530369)

<sup>1835</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=530659](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=530659)

<sup>1836</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=566479](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=566479)

<sup>1837</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=564299](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=564299)

<sup>1838</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=566694](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=566694)

### 1.178. rhnsd

#### 1.178.1. RHBA-2009:1655: bug fix update



##### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2009:1655](#)<sup>1839</sup>

An updated rhnsd package that fixes a problem with inconsistent system environments during rhn\_check execution is now available.

The Red Hat Update Agent -- rhnsd -- periodically polls the Red Hat Network (RHN) or a Red Hat Network Satellite server to determine actions to be executed on a client, such as which packages need to be updated on a given system, and then runs those actions.

This update addresses the following issue:

\* an alternative to polling a server for scheduled actions is pushing the scheduled actions from the RHN or Satellite server to the client. This is implemented with the XMPP protocol and the OSAD program running on a client. Both rhnsd and osad use the rhn\_check program to execute scheduled actions on a client. Previously, the system environment passed to rhn\_check by rhnsd was not consistent with the system environment passed to rhn\_check by osad. In some circumstances, this inconsistency led to update failures. With this update both rhnsd and osad now return an equivalent "env" to rhn\_check and actions executed either by pulling (rhnsd) or pushing (osad) both work as expected. ([BZ#503738](#)<sup>1840</sup>)

All RHN or RHN Satellite users should install this updated package which fixes this bug.

### 1.179. rhppl

#### 1.179.1. RHBA-2010:0318: bug fix update

An updated rhppl package that fixes two bugs is now available

The rhppl package contains a Python library for configuring and running the X Window System.

This updated package fixes the following bugs:

\* The American Megatrends Inc. KVM cannot be handled by the standard mouse driver. It needs a configuration section in xorg.conf to employ the evdev driver instead. This issue was resolved by parsing the list of available devices and adding the configuration section on demand. ([BZ#492565](#)<sup>1841</sup>)

\* The list of screen resolutions was not emptied in set\_resolution causing some resolutions to not be selectable. An initialization variable has now been implemented. This allows the correct screen resolutions choices. ([BZ#242577](#)<sup>1842</sup>)

---

<sup>1840</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=503738](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=503738)

<sup>1841</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=492565](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=492565)

<sup>1842</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=242577](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=242577)

Users of rhppl are advised to upgrade to this updated package, which resolves these issues.

## 1.180. rsyslog

### 1.180.1. RHBA-2010:0213: bug fix update

An updated rsyslog package that fixes various bugs and adds enhancements are now available.

The rsyslog package is an enhanced, multi-threaded syslog daemon. It supports MySQL, syslog/TCP, RFC 3195, permitted sender lists, filtering on any message part, and fine grain output format control. It is compatible with stock syslogd and can be used as a drop-in replacement. Rsyslog is simple to set up, with advanced features suitable for enterprise-class, encryption-protected syslog relay chains.

rsyslog has been rebased to upstream version 3.22.1-3. The rebased package provides fixes for the following bugs:

\* when rsyslog had directories creation disabled with \$CreateDirs off, regular file creation was also disabled. This resulted in a situation where directory creation needed to be enabled to allow regular file creation. File creation is now allowed in existing directories, even while directory creation is disabled. ([BZ#473419](https://bugzilla.redhat.com/show_bug.cgi?id=473419)<sup>1843</sup>)

\* if remote messages were being queued, the local rsyslog daemon would stop logging when messages were being discarded or if TCP connections were being rejected. This also caused some applications to fail. The configuration details were updated, and local messages now continue being logged, even when remote messages are queued. ([BZ#519201](https://bugzilla.redhat.com/show_bug.cgi?id=519201)<sup>1844</sup> & [BZ#519203](https://bugzilla.redhat.com/show_bug.cgi?id=519203)<sup>1845</sup>)

These rebased packages also provide the following enhancements:

\* rsyslog can now handle a greater number of clients. ([BZ#475217](https://bugzilla.redhat.com/show_bug.cgi?id=475217)<sup>1846</sup>)

\* support has been added for Transport Layer Security (TLS) encryption and conditional filters. ([BZ#488068](https://bugzilla.redhat.com/show_bug.cgi?id=488068)<sup>1847</sup>)

\* timezone conversion support has been added. All rsyslog messages should now appear in local time. ([BZ#499186](https://bugzilla.redhat.com/show_bug.cgi?id=499186)<sup>1848</sup>)

\* the rsyslog server can now handle more than 1000 open files and Transmission Control Protocol (TCP) connections. ([BZ#519192](https://bugzilla.redhat.com/show_bug.cgi?id=519192)<sup>1849</sup>)

All users of rsyslog are advised to upgrade to these updated packages, which resolve these issues and add these enhancements.

---

<sup>1843</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=473419](https://bugzilla.redhat.com/show_bug.cgi?id=473419)

<sup>1844</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=519201](https://bugzilla.redhat.com/show_bug.cgi?id=519201)

<sup>1845</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=519203](https://bugzilla.redhat.com/show_bug.cgi?id=519203)

<sup>1846</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=475217](https://bugzilla.redhat.com/show_bug.cgi?id=475217)

<sup>1847</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=488068](https://bugzilla.redhat.com/show_bug.cgi?id=488068)

<sup>1848</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=499186](https://bugzilla.redhat.com/show_bug.cgi?id=499186)

<sup>1849</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=519192](https://bugzilla.redhat.com/show_bug.cgi?id=519192)

## 1.181. ruby

### 1.181.1. RHBA-2010:0012: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2010:0012](#)<sup>1850</sup>

Updated ruby packages that fix a regression are now available.

Ruby is an extensible, interpreted, object-oriented, scripting language. It has features to process text files and to do system management tasks.

These updated ruby packages fix the following bug:

\* a regression introduced by the fix for [CVE-2009-1904](#)<sup>1851</sup> caused leading zeros after the decimal point in BigDecimal objects to be dropped, which could have led to incorrect mathematical calculations. This update fixes this problem by ensuring that leading zeros following a decimal point in BigDecimal objects are not dropped.

A link to the update which introduced this regression is provided in the References section of this errata. ([BZ#546245](#)<sup>1852</sup>)

All users of ruby are advised to upgrade to these updated packages, which resolve this issue.

## 1.182. samba

### 1.182.1. RHBA-2009:1641: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1641](#)<sup>1853</sup>

Updated samba packages that fix credentials file handling for mount.cifs are now available for Red Hat Enterprise Linux 5.

Samba is a suite of programs used by machines to share files, printers, and other information.

The kernel CIFS client mount helper binary (mount.cifs) uses details stored in a credentials file to authenticate with file servers. After a recent security update, mount.cifs no longer parsed credentials files correctly, and included trailing newlines in the authentication information. Attempts to authenticate would therefore fail with errors such as NT\_STATUS\_LOGON\_FAILURE. The parsing code is now corrected and no longer includes the newline as part of the authentication details. Mount.cifs can therefore use credentials files to authenticate with file servers successfully.

---

<sup>1851</sup> <https://www.redhat.com/security/data/cve/CVE-2009-1904.html>

<sup>1852</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=546245](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=546245)

Users of Samba should upgrade to these updated packages, which contain backported patches to correct this issue.

## 1.182.2. RHSA-2009:1529: Moderate security update



### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2009:1529](#)<sup>1854</sup>

Updated samba packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

Samba is a suite of programs used by machines to share files, printers, and other information.

A denial of service flaw was found in the Samba `smbd` daemon. An authenticated, remote user could send a specially-crafted response that would cause an `smbd` child process to enter an infinite loop. An authenticated, remote user could use this flaw to exhaust system resources by opening multiple CIFS sessions. ([CVE-2009-2906](#)<sup>1855</sup>)

An uninitialized data access flaw was discovered in the `smbd` daemon when using the non-default "dos filemode" configuration option in "smb.conf". An authenticated, remote user with write access to a file could possibly use this flaw to change an access control list for that file, even when such access should have been denied. ([CVE-2009-1888](#)<sup>1856</sup>)

A flaw was discovered in the way Samba handled users without a home directory set in the back-end password database (e.g. `/etc/passwd`). If a share for the home directory of such a user was created (e.g. using the automated "[homes]" share), any user able to access that share could see the whole file system, possibly bypassing intended access restrictions. ([CVE-2009-2813](#)<sup>1857</sup>)

The `mount.cifs` program printed CIFS passwords as part of its debug output when running in verbose mode. When `mount.cifs` had the `setuid` bit set, a local, unprivileged user could use this flaw to disclose passwords from a file that would otherwise be inaccessible to that user. Note: `mount.cifs` from the samba packages distributed by Red Hat does not have the `setuid` bit set. This flaw only affected systems where the `setuid` bit was manually set by an administrator. ([CVE-2009-2948](#)<sup>1858</sup>)

Users of Samba should upgrade to these updated packages, which contain backported patches to correct these issues. After installing this update, the `smb` service will be restarted automatically.

## 1.182.3. RHBA-2010:0300: bug fix update

Updated samba packages that contain various bugfixes are now available.

Samba is a suite of programs used by machines to share files, printers, and other information.

<sup>1855</sup> <https://www.redhat.com/security/data/cve/CVE-2009-2906.html>

<sup>1856</sup> <https://www.redhat.com/security/data/cve/CVE-2009-1888.html>

<sup>1857</sup> <https://www.redhat.com/security/data/cve/CVE-2009-2813.html>

<sup>1858</sup> <https://www.redhat.com/security/data/cve/CVE-2009-2948.html>

This package addresses the following bugs:

\* previously, the man pages and usage messages for rpcclient, smbcacls, samba-client, smbget, smbtree, and pdbedit contained errors, omissions, and outdated information. Users could not therefore rely on the provided documentation to use these programs. The documentation for each of these components has been reviewed and corrected and no longer contains misleading information.

([BZ#457082](https://bugzilla.redhat.com/show_bug.cgi?id=457082)<sup>1859</sup>,

[BZ#457096](https://bugzilla.redhat.com/show_bug.cgi?id=457096)<sup>1860</sup>, [BZ#457097](https://bugzilla.redhat.com/show_bug.cgi?id=457097)<sup>1861</sup>, [BZ#457192](https://bugzilla.redhat.com/show_bug.cgi?id=457192)<sup>1862</sup>, [BZ#457195](https://bugzilla.redhat.com/show_bug.cgi?id=457195)<sup>1863</sup>, [BZ#457203](https://bugzilla.redhat.com/show_bug.cgi?id=457203)<sup>1864</sup>, [BZ#457384](https://bugzilla.redhat.com/show_bug.cgi?id=457384)<sup>1865</sup>,

[BZ#457385](https://bugzilla.redhat.com/show_bug.cgi?id=457385)<sup>1866</sup>)

\* Samba stores its own Kerberos configuration in `/var/cache/samba/smb_krb5`. Previously, although the "net ads join" command used this configuration and was able to join an Active Directory, "net ads testjoin" and "net ads leave" ignored the samba- specific file and tried to use the configuration in `/etc/krb5.conf` instead. These commands would therefore fail when authentication through Kerberos was needed. "net ads testjoin" and "net ads leave" now use `/var/cache/samba/smb_krb5` and therefore work with authenticated Active Directory resources. ([BZ#509170](https://bugzilla.redhat.com/show_bug.cgi?id=509170)<sup>1867</sup>)

\* `cifs.upcall` performs certain CIFS-related tasks for the kernel in user space. The version of `cifs.upcall` included with previous versions of Samba could not provide the kernel with the credentials cache path stored in the `KRB5CCNAME` environment variable. Attempts to mount CIFS shares through `fstab` as a normal user would therefore fail. The version of `cifs.upcall` included with Red Hat Enterprise Linux 5.5 can now provide the kernel with the credentials cache path, and CIFS shares can therefore be mounted for normal users. ([BZ#517195](https://bugzilla.redhat.com/show_bug.cgi?id=517195)<sup>1868</sup>)

\* previously, when handling a POSIX open call, Samba did not account for the `SMB_O_CREAT`, `SMB_O_EXCL`, or `SMB_O_TRUNC` flags. As a result, Samba would respond with `STATUS_INVALID_PARAMETER` to any of these flags instead of honoring the call. Samba now recognizes these flags and honors POSIX open calls that use them. ([BZ#522866](https://bugzilla.redhat.com/show_bug.cgi?id=522866)<sup>1869</sup>)

\* when setting the "allow trusted domain = no" parameter on a Samba server it would not have any effect on the configuration and Samba would still attempt to contact trusted domains. By refreshing the trusted domain cache only if the parameter "allow trusted domain = yes" is set, Samba no longer attempts to contact trusted domains when "allow trusted domain = no". ([BZ#526065](https://bugzilla.redhat.com/show_bug.cgi?id=526065)<sup>1870</sup>)

\* `mount.cifs` would fail to correctly authenticate when a credentials file was used. As a result, any mount operation that used a credentials file would fail. By correcting the newlines during the parsing routines during mounting the issue has been fixed. `mount.cifs` now works correctly when authenticating with a credentials file. ([BZ#532153](https://bugzilla.redhat.com/show_bug.cgi?id=532153)<sup>1871</sup>)

\* mounting and unmounting a CIFS filesystem quickly would eventually lead to the CIFS mounts becoming unmountable. The issue has been corrected by linking `mtab.o` to the building of `mount.cifs`

---

<sup>1859</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=457082](https://bugzilla.redhat.com/show_bug.cgi?id=457082)

<sup>1860</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=457096](https://bugzilla.redhat.com/show_bug.cgi?id=457096)

<sup>1861</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=457097](https://bugzilla.redhat.com/show_bug.cgi?id=457097)

<sup>1862</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=457192](https://bugzilla.redhat.com/show_bug.cgi?id=457192)

<sup>1863</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=457195](https://bugzilla.redhat.com/show_bug.cgi?id=457195)

<sup>1864</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=457203](https://bugzilla.redhat.com/show_bug.cgi?id=457203)

<sup>1865</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=457384](https://bugzilla.redhat.com/show_bug.cgi?id=457384)

<sup>1866</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=457385](https://bugzilla.redhat.com/show_bug.cgi?id=457385)

<sup>1867</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=509170](https://bugzilla.redhat.com/show_bug.cgi?id=509170)

<sup>1868</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=517195](https://bugzilla.redhat.com/show_bug.cgi?id=517195)

<sup>1869</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=522866](https://bugzilla.redhat.com/show_bug.cgi?id=522866)

<sup>1870</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=526065](https://bugzilla.redhat.com/show_bug.cgi?id=526065)

<sup>1871</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=532153](https://bugzilla.redhat.com/show_bug.cgi?id=532153)



and unmount.cifs. CIFS mounts no longer become unmountable when performing quick mounting and unmounting of the filesystem. ([BZ#533912](https://bugzilla.redhat.com/show_bug.cgi?id=533912)<sup>1872</sup>)

\* kdebase conflicted with Samba 3. Samba 2 components libsmbclient and libsmbclient-devel are now available as independent rpms and can be installed alongside Samba 3. By separating out these packages it allows for kdebase to reference its dependencies independent of a Samba installation, correcting the conflict. ([BZ#555654](https://bugzilla.redhat.com/show_bug.cgi?id=555654)<sup>1873</sup>)

Users of Samba should upgrade to these updated packages, which resolve these issues.

## 1.183. samba3x

### 1.183.1. RHBA-2010:0301: bug fix update

Updated samba3x packages that contain various bug fixes are now available for Red Hat Enterprise Linux 5.

Samba is a suite of programs used to share files, printers and other information between machines.

These packages contain fixes for the following bugs:

\* the upstream Samba version in the samba3x packages distributed with the RHEA-2009:1399 update contained broken implementations of the Netlogon credential chain and SAMR access checks security subsystems. This prevented Samba from acting as a domain controller: Client systems could not join the domain; users could not authenticate; and systems could not access the user and group list. ([BZ#506292](https://bugzilla.redhat.com/show_bug.cgi?id=506292)<sup>1874</sup>)

\* to modify the access control list for a file, WRITE\_DAC and WRITE\_OWNER access must be requested when the file is opened. When dos\_filemode was enabled, these requests were not sent, so the access control list for a writeable file could not be changed. WRITE\_DAC and WRITE\_OWNER access are now requested when dos\_filemode is enabled, so the access control list can be modified. ([BZ#537165](https://bugzilla.redhat.com/show_bug.cgi?id=537165)<sup>1875</sup>)

\* samba3x was previously available only for AMD64 and Intel 64 architectures. It is now available for Itanium, PowerPC, IBM System z, x86, AMD64 and Intel 64 server and client variants. ([BZ#547715](https://bugzilla.redhat.com/show_bug.cgi?id=547715)<sup>1876</sup>)

\* cifs.upcall could not determine the KRB5CCNAME environment variable, so it could not locate a Kerberos credential cache with a non-default name. This caused a 'required key not available' error when attempting to mount a Common Internet File System (CIFS) share. cifs.upcall now scans the /tmp directory for credential caches with non-default names, enabling users authenticated via pam\_krb5 to use their tickets to mount CIFS. ([BZ#548129](https://bugzilla.redhat.com/show_bug.cgi?id=548129)<sup>1877</sup>)

\* samba3x was previously only available as a technology preview for AMD64 and Intel 64 architectures. It is now supported for Itanium, PowerPC, IBM System z, x86, AMD64 and Intel 64 server and client variants.

---

<sup>1872</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=533912](https://bugzilla.redhat.com/show_bug.cgi?id=533912)

<sup>1873</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=555654](https://bugzilla.redhat.com/show_bug.cgi?id=555654)

<sup>1874</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=506292](https://bugzilla.redhat.com/show_bug.cgi?id=506292)

<sup>1875</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=537165](https://bugzilla.redhat.com/show_bug.cgi?id=537165)

<sup>1876</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=547715](https://bugzilla.redhat.com/show_bug.cgi?id=547715)

<sup>1877</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=548129](https://bugzilla.redhat.com/show_bug.cgi?id=548129)

Important: Clustered samba3x support is still a technology preview, and is available only on AMD64 and Intel 64 systems. ([BZ#557921](https://bugzilla.redhat.com/show_bug.cgi?id=557921)<sup>1878</sup>)

\* Using the Windows Add Printer Wizard on samba3x-3.3.8 with CUPS configuration led to SMB panic. The printer would be installed correctly on CUPS. On Windows clients, an error message printed due to a Windows driver issue, installation failed, and SMB panic would be printed in the log. This patch resolves the SMB panic issue, allowing printers to be installed and removed from samba3x in Windows clients. ([BZ#571778](https://bugzilla.redhat.com/show_bug.cgi?id=571778)<sup>1879</sup>)

All previous samba3x technology preview packages must be removed before installing this new supported version of samba3x.

All users are advised to upgrade to these updated packages, which fix these bugs.

## 1.184. sblim

### 1.184.1. RHBA-2010:0231: bug fix and enhancement update

Updated sblim packages that fix various bugs and add various enhancements are now available.

SBLIM stands for Standards-Based Linux Instrumentation for Manageability. It consists of a set of standards-based, Web-Based Enterprise Management (WBEM) modules that use the Common Information Model (CIM) standard to gather and provide systems management information, events, and methods to local or networked consumers via an CIM object services broker using the CMPI (Common Manageability Programming Interface) standard. This package provides a set of core providers and development tools for systems management applications.

These packages address the following bugs:

\* The libraries installed with sblim-cmpi-base were assigned incorrect permissions. This meant that any user outside of a specific group could not read the packages, forcing the check for the SBLIM Base in sblim-sfcb to fail. To fix this bug, when the libraries are installed the assigned permissions allow for any user group to access them. The library files are now able to be used in the building of other packages. ([BZ#526756](https://bugzilla.redhat.com/show_bug.cgi?id=526756)<sup>1880</sup>)

\* Some sblim packages were released with the incorrect version number. This did not cause any error in installation or the running of the components. For consistency in file naming conventions and to improve package management, the version numbers of all sblim packages now reflect the correct version numbers. ([BZ#516785](https://bugzilla.redhat.com/show_bug.cgi?id=516785)<sup>1881</sup>)

As well, these updated packages add the following enhancements:

\* A new sblim-smis-hba package has been added to the SBLIM package set. This package adds the Host Bus Adapters (HBA) API that is an industry standard C language for management of fibre channel host bus adapters and discovery of SAN resources. ([BZ#512238](https://bugzilla.redhat.com/show_bug.cgi?id=512238)<sup>1882</sup>)

---

<sup>1878</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=557921](https://bugzilla.redhat.com/show_bug.cgi?id=557921)

<sup>1879</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=571778](https://bugzilla.redhat.com/show_bug.cgi?id=571778)

<sup>1880</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=526756](https://bugzilla.redhat.com/show_bug.cgi?id=526756)

<sup>1881</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=516785](https://bugzilla.redhat.com/show_bug.cgi?id=516785)

<sup>1882</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=512238](https://bugzilla.redhat.com/show_bug.cgi?id=512238)

\* A new sblim-sfcb package has been added to the SBLIM package set. This package adds the Small Footprint CIM Broker (SFCB). The SFCB allows for improved standardized Linux Systems Management in terms of a CIM and WEBM infrastructure between linux distributions. ([BZ#512370](#)<sup>1883</sup>)

\* A new sblim-sfcc package has been added to the SBLIM package set. This package adds the Small Footprint CIM Client (SFCC). The SFCC provides a client that can directly access the SFCB in order to add a CIM to your programs. ([BZ#512374](#)<sup>1884</sup>)

\* These packages include the upgrade of many SBLIM packages to the latest upstream versions. These upgrades fix bugs and add KVM support and CMPI 2.0 compliance. ([BZ#512230](#)<sup>18861885</sup>)


\* The license for all SBLIM packages has been changed to EPL. ([BZ#512230](#)<sup>18881887</sup>,

[BZ#512369](#)<sup>1889</sup>)

Users are advised to upgrade to these updated sblim packages, which resolve these issues and add these enhancements.

## 1.185. screen

### 1.185.1. RHBA-2009:1621: bug fix update



**Note**  
This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1621](#)<sup>1890</sup>

An updated screen package that fixes a bug is now available.

The screen utility allows multiple logins on a single terminal. Screen is useful for users who telnet into a machine or are connected via a dumb terminal, but want to use more than one login.

This updated package resolves the following issue:

\* in the previous screen release, utempter support was disabled. The utempter library provides an interface for terminal emulators such as screen and xterm to record user sessions to utmp and wtmp files. Without utempter support, commands such as logname and "who am i" did not work in screen sessions. With this update the screen spec file was updated to require the libutempter-devel package. This ensures utempter support is enabled and commands such as logname, "who am i" and "w" work in screen sessions as expected. ([BZ#541875](#)<sup>1891</sup>)

All screen users are advised to upgrade to this updated package, which resolves this issue.

<sup>1883</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=512370](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=512370)

<sup>1884</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=512374](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=512374)

<sup>1886</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=512230](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=512230)

<sup>1885</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=512230](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=512230)

<sup>1888</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=512230](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=512230)

<sup>1887</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=512230](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=512230)

<sup>1889</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=512369](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=512369)

<sup>1891</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=541875](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=541875)

### 1.186. scsi-target-utils

#### 1.186.1. RHBA-2010:0067: bug fix and enhancement update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2010:0067](#)<sup>1892</sup>

An updated `scsi-target-utils` package that fixes various bugs is now available.

The `scsi-target-utils` package contains the daemon and tools to set up and monitor SCSI targets. Currently, iSCSI software and iSER targets are supported.

This updated `scsi-target-utils` package includes fixes for the following bugs:

\* the `tgtadm` utility is used to monitor and modify SCSI target software. When using `tgtadm` to present an LVM-backed target to clients, attempting to create a new file system by running the `mkfs` utility on a logical volume caused the `tgtd` daemon to become unresponsive and connection errors to be logged to `/var/log/messages`. With this update, clients are once again able to successfully create a new file system on an LVM logical volume. ([BZ#545785](#)<sup>1893</sup>)

\* running the command `"tgtadm --mode connection --op delete"` to instruct `tgtadm` to close and remove an open connection to a target which has ongoing I/O caused the `tgtadm` utility to segmentation fault. Subsequently, attempting to stop the `tgtd` daemon by running `"service tgtd stop"` failed and resulted in error messages. With this update, it is now possible to use `tgtadm` to close and remove an open connection to a target which is undergoing I/O without causing `tgtadm` to crash, and subsequently stopping or restarting the `tgtd` service proceeds as expected. ([BZ#545786](#)<sup>1894</sup>)

\* attempting to create 32 or more iSCSI targets using `tgtadm` caused the utility to segmentation fault after successfully creating the first 31 targets. This update fixes this limitation so that `tgtadm` does not segmentation fault when creating large numbers of targets, such as 400 or more. ([BZ#552928](#)<sup>1895</sup>)

\* the `/etc/tgt/targets.conf` file now supports more advanced configuration parameters. Refer to the `tgtd-admin(8)` manual page for further information about valid parameters for the `/etc/tgt/targets.conf` file.

All users of `scsi-target-utils` are advised to upgrade to this updated package, which resolves these issues.

---

<sup>1893</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=545785](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=545785)

<sup>1894</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=545786](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=545786)

<sup>1895</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=552928](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=552928)

## 1.187. selinux-policy

### 1.187.1. RHBA-2009:1495: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata *RHBA-2009:1495*<sup>1896</sup>

Updated selinux-policy packages that fix a bug are now available.

The selinux-policy packages contain the rules that govern how confined processes run on the system.

These updated packages fix the following bug:

\* the cyrus-imapd daemon is compiled with net-snmp support and it attempts to register its snmp sub-agent during startup. This was not allowed by previous SELinux policy. These updated packages include updated policy that allows cyrus-imapd to register its snmp sub-agent during startup, as expected. ([BZ#523548](#)<sup>1897</sup>)

All users are advised to upgrade to these updated packages, which resolves these issue.

### 1.187.2. RHBA-2010:0013: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata *RHBA-2010:0013*<sup>1898</sup>

Updated selinux-policy packages that fix several bugs are now available.

The selinux-policy packages contain the rules that govern how confined processes run on the system.

These updated selinux-policy packages provide fixes for the following bugs:

\* the "setkey" utility from the ipsec-tools package manipulates and dumps the kernel's Security Policy Database (SPD) entries and Security Association Database (SAD) entries. The current selinux-policy did not allow users running under the "sysadm" role to use setkey. This update allows users running under the sysadm SELinux role to use the setkey utility from the ipsec-tools package. ([BZ#538449](#)<sup>1899</sup>)

\* using the Openswan implementation of IPsec could have resulted in AVC (Access Vector Cache) denials causing the integrity check to fail, which in turn would cause the pluto key management daemon not to start. This update includes updated policy rules for IPsec which fix the AVC denials so that pluto is allowed to run as expected. Note that this is necessary for FIPS-140 compliance. ([BZ#538452](#)<sup>1900</sup>)

<sup>1897</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=523548](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=523548)

<sup>1899</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=538449](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=538449)

<sup>1900</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=538452](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=538452)

\* SELinux denials caused by the ssh-keygen's "system\_u:object\_r:initrc\_exec\_t" context caused ssh-keygen to fail to generate public/private RSA key pairs. These updated SELinux policy rules allow ssh-keygen to successfully generate public/private RSA key pairs as expected. ([BZ#538453](#)<sup>1901</sup>)

\* when the "ifup" script was run manually in order to activate the first IPsec interface, which then attempts to start racoon, racoon incorrectly ran under the "unconfined\_t" context instead of under the expected "racoon\_t", thus preventing it from starting. Note that this did not happen when the IPsec network interface configuration file contained an "ONBOOT=yes" parameter; racoon successfully started in this case. With this update, racoon possesses the correct context, "racoon\_t", which allows it to run when started via the ifup network startup script. ([BZ#538503](#)<sup>1902</sup>)

All users are advised to upgrade to these updated packages, which resolve these issues.

### 1.187.3. RHBA-2010:0063: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2010:0063](#)<sup>1903</sup>

Updated selinux-policy packages that fix a regression that prevented postfix-driven systems from sending e-mail via sendmail are now available.

The selinux-policy packages contain the rules that govern how confined processes run on the system.

These updated selinux-policy packages provide the fix for the following bug:

\* selinux-policy errata update RHBA-2010:0013 introduced a regression which prevented postfix-driven systems from sending e-mail using sendmail if SELinux was in enforcing mode. With this update, postfix\_postdrop can read and write sendmail unix\_stream\_sockets, correcting the regression and allowing e-mails to be sent using sendmail. ([BZ#555793](#)<sup>1904</sup>)

Note: a workaround involving the manual creation of a mypostfix.te was documented in [BZ#553492](#)<sup>1905</sup> (see References below). Once this update is installed, the workaround and manually created file are no longer required.

All users should upgrade to these updated packages, which resolve this issue.

### 1.187.4. RHBA-2010:0182: bug fix update

Updated **selinux-policy** packages that fix numerous bugs are now available.

The selinux-policy packages contain the rules that govern how confined processes run on the system.

These updated selinux-policy packages contain the following changes to SELinux policy rules:

- The **coolkey** library used by some Kerberos implementations caused an SELinux denial when credentials were sent to an NFS server, and during the creation of a cache directory. This package modifies SELinux policy so that the coolkey Kerberos library is excluded from being audited when performing this operation. ([BZ#294651](#)<sup>1906</sup>)

---

<sup>1901</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=538453](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=538453)

<sup>1902</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=538503](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=538503)

<sup>1904</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=555793](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=555793)

<sup>1905</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=553492](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=553492)

- A leaked file descriptor in **cupsd** caused an SELinux error or denial. SELinux policy has been modified to allow this activity and not to cause a denial when this activity takes place. ([BZ#483395](#)<sup>1907</sup>)
- The **/root/.ssh** directory contained incorrect SELinux permissions if it was deleted and re-created. This permission error caused the **ssh-keygen** command to fail when creating keys in this directory from an init script, as it was not labelled correctly. SELinux policy has been modified to enable the correct permissions on the **/root/.ssh** directory if it is removed and re-added. Having the correct permission on this directory results in **ssh-keygen** now being able to successfully generate keys as expected. ([BZ#492519](#)<sup>1908</sup>)
- Hosts with SELinux in enforcing mode were not able to create a cluster with Red Hat Cluster Suite (RHCS) when running **service cman start** because **aisexec** could not allocate shared memory. Support has been added in SELinux policy for Cluster Suite, which resolves these issues. ([BZ#503141](#)<sup>1909</sup>)
- An SELinux denial was triggered when the **coolkey** command integrated with **samba** to join an Active Directory service. SELinux policy has been modified to allow for proper coolkey cache management in the samba policy module. ([BZ#507797](#)<sup>1910</sup>)
- SELinux policy has been modified to allow proper operation of the **rsync** command when it is used via the SSH protocol. ([BZ#510748](#)<sup>1911</sup>)
- A problematic library file for the Oracle **sqlplus** command caused an SELinux denial. Policy has been modified to label this file correctly to allow for its unexpected behavior. The sqlplus command functions normally after applying this update. ([BZ#512375](#)<sup>1912</sup>)
- Users operating in the **sysadm** SELinux role can now use the **setkey** utility from the **ipsec-tools** package. ([BZ#513447](#)<sup>1913</sup>)
- A transition rule has been added to SELinux policy that allows **vbetool** the permissions it needs to operate normally. ([BZ#515491](#)<sup>1914</sup>)
- When **setkey** was executed from a network startup script, an SELinux denial was triggered. An interface has been added to enable integration with temporary files when using setkey within the MLS SELinux policy. ([BZ#515687](#)<sup>1915</sup>)
- The protection offered over the **rsync** command has changed. rsync is now protected only when started from inetd or xinetd. Other usages of rsync are considered client-side operations and are not protected any further than that of utilities such as **cp** or **scp**. ([BZ#516780](#)<sup>1916</sup>)
- The **sudo** command was not properly launching an intermediary shell to authenticate users with correct sudo role privileges. This fix allows transitions to operate normally and allows users to execute commands as root via sudo, when configured to do so. ([BZ#519017](#)<sup>1917</sup>)
- Launching an **ipsec** connection by using the **service network restart** command did not succeed. The ipsec connection did not start as it was started from the **init\_t** domain. Policy for **setkey** has been modified so that it can now read temporary data from init scripts, and ipsec connections now start normally from the **init\_t** domain. ([BZ#519363](#)<sup>1918</sup>)
- Scripts for **mod\_fcgid**, a CGI plugin for the Apache HTTP server caused SELinux permission errors when used. Policy has been modified to both allow **mod\_fcgid** scripts the required permissions, and to allow CGI applications to use their own mail modules to send mail, instead of calling **sendmail**. ([BZ#519369](#)<sup>1919</sup>)



- Instances of `#!/usr/bin/env python` have been removed from SELinux policy source code, as using this technique to call `python` in the top of an executable python file is being discontinued by Red Hat developers. ([BZ#521284](#)<sup>1920</sup>)
- Support for Red Hat Cluster Suite has been added to SELinux policy. Please note that SELinux policy only provides coverage for the infrastructure components. Services directly managed by Cluster Suite will require their own policies and are not covered by this enhancement. ([BZ#522158](#)<sup>1921</sup>)
- SELinux policy has been modified so that `cyrus-imapd` is now able to register its SNMP sub-agent by connecting to a socket upon startup. ([BZ#523548](#)<sup>1922</sup>)
- An SELinux denial was triggered when configuring the `SNMP` daemon to listen on TCP or UDP ports for AgentX sub-agents. Policy has been modified so that this daemon can now bind TCP/UDP sockets to AgentX ports. ([BZ#523773](#)<sup>1923</sup>)
- SELinux denials were caused when implementing user quotas over `NFS` (Network File System) shares. Policy has been modified to properly allow for the normal operation of quotas when using NFS shares. ([BZ#525420](#)<sup>1924</sup>)
- Upon updating the `udev` daemon to the latest version and restarting it, the SELinux context for `udev` was changed from the default, causing errors. This update ensures that this context remains correct when restarting `udev`. ([BZ#526640](#)<sup>1925</sup>)
- SELinux policy has been modified to not trigger an error when the `virDomainSave()` API is called from `qemu-kvm`. ([BZ#530552](#)<sup>1926</sup>)
- `procmail` was causing an AVC denial when attempting to read files used by `spamassassin`. Rules have been added to policy so that these applications can communicate normally via pipes. ([BZ#530750](#)<sup>1927</sup>)
- The ability to send and receive unlabeled packets was added to policy rules. ([BZ#530809](#)<sup>1928</sup>)
- A bug prevented the installation of the `selinux-policy-strict` package because the requirements of `aisexec` were not properly met. The strict policy can now be installed as expected. ([BZ#531196](#)<sup>1929</sup>)
- Real Time Kernel support was added to `selinux-policy`. ([BZ#531230](#)<sup>1930</sup>)
- The `e4fsck` command was not properly labeled, causing execution to fail. Policy permissions have been fixed so that `e4fsck` is now correctly labeled. ([BZ#532565](#)<sup>1931</sup>)
- Permissions were modified to allow `pluto` to write logs properly. ([BZ#537106](#)<sup>1932</sup>)
- This update includes updated policy rules for `IPsec`, fixing the AVC denials that prevented `pluto` from running properly. After applying this update, `pluto` runs as expected. Note that this is necessary for FIPS-140 security compliance. ([BZ#537133](#)<sup>1933</sup>)
- `vhostmd` is a daemon that provides a communication channel between a host and its hosted virtual machines. Implementing a `vhostmd` daemon caused AVC denial errors when launching it via `service vhostmd start`. SELinux policy rules have been added to protect the `vhostmd` daemon. The daemon starts and operates normally after applying the update. ([BZ#543941](#)<sup>1934</sup>)

- SELinux AVC denial errors were triggered when using the sysadm SELinux user to connect to **raccoon** using a UNIX domain stream socket. After applying this update, access functions as expected. ([BZ#545369](#)<sup>1935</sup>)
- When using the MLS functionality, **iptables** can now start properly and has proper permissions to read configuration files. ([BZ#546604](#)<sup>1936</sup>)
- Policy has been modified to give the **smartd** daemon the ability to read from and write to generic SCSI devices. ([BZ#547387](#)<sup>1937</sup>)
- SELinux policy has been modified to fix a segfault error when using an iSCSI target with the **bnx2i** interface type. ([BZ#548599](#)<sup>1938</sup>)
- The **/var/vdsm** directory was incorrectly labeled by SELinux, showing two different SELinux contexts. After applying this update, the directory is now correctly labeled with a single label. ([BZ#549492](#)<sup>1939</sup>)
- When using the '-i' option to the **lpadmin** command to set an interface script for a printer, SELinux error messages are triggered. A new type, **cupsd\_interface\_t**, has been added to policy to allow **cupsd** to properly utilize a System V style interface script. ([BZ#550015](#)<sup>1940</sup>)
- The **postgresql** regression tests include libraries that need to be dynamically loaded by the postgresql server. Some of these libraries were incorrectly labeled, which caused the regression tests to fail and SELinux errors to appear. This update applies the correct permissions to the libraries, and the postgresql regression tests now operate as expected. ([BZ#551063](#)<sup>1941</sup>)
- **prelink** is a utility that can reduce the startup times of applications by linking to libraries and storing the linking in the executable. prelink is now allowed under SELinux policy to load and execute functions from shared libraries, with legacy support included for older libraries. ([BZ#551664](#)<sup>1942</sup>)
- **qemu-kvm** caused SELinux errors when creating or starting a virtual machine when **Transport Layer Security** (TLS) is enabled in qemu.conf for an environment using a Public Key Infrastructure (PKI). This error occurred because qemu-kvm did not have sufficient permission to read from a random number generator (**/dev/random** and **/dev/urandom**) in order to gather its entropy. Permissions have been modified so that qemu-kvm can now read from these random number generators. ([BZ#552763](#)<sup>1943</sup>)
- A regression error was discovered when installing new SELinux packages. The **postfix\_postdrop** command was unable to use sockets. This resulted in emails not being sent. After applying this update, postfix is able to read and write sendmail unix\_stream\_sockets and emails can be sent using sendmail as expected. ([BZ#553492](#)<sup>1944</sup>)
- The **/etc/xen** was incorrectly labeled. This caused errors when using automated scripts for staging Xen guest virtual machines. A fix was applied to correctly label the directory, which resolved the problem. Xen guests are now functioning as expected. ([BZ#554777](#)<sup>1945</sup>)
- Restarting networking services using the **service network restart** command resulted in an AVC denial caused by dhcpcd\_t being unable to relabel to and from net\_conf\_t. This update allows this with the result that restarting networking succeeds without SELinux denials. ([BZ#559355](#)<sup>1946</sup>)
- The **iscsid** daemon, which implements the control path of the iSCSI protocol along with management functions, could not create its log file due to an incorrect SELinux context. ([BZ#562303](#)<sup>1947</sup>)

- The context for the named name server daemon, when running in a chrooted environment, was incorrect, and with this update is labeled correctly. ([BZ#562833](#)<sup>1948</sup>)
- Attempting to save the firewall configuration with the **service iptables save** command triggered an AVC denial. This update changes the default context for the **/sbin/iptables-save** application to `iptables_exec_t` so that the firewall configuration can be saved. ([BZ#564376](#)<sup>1949</sup>)
- Attempting to run a CGI script from a **cgi-bin** directory mounted on an NFS share resulted in an AVC denial, whereas serving static pages from a **public\_html** directory worked as expected. CGI scripts can now be run from NFS-mounted directories given the correct permissions. ([BZ#566557](#)<sup>1950</sup>)
- When the SELinux boolean `ftp_home_dir` was enabled, the `allow_ftpd_anon_write` boolean did not take effect, and users could upload files to their home directories via anonymous FTP even though write access should have been restricted by the value of `allow_ftpd_anon_write`. With this update, the value of `allow_ftpd_anon_write` allows or permits anonymous FTP writes, as expected. ([BZ#566975](#)<sup>1951</sup>)

All users are advised to upgrade to these updated packages, which resolve these issues.

## 1.188. sendmail

### 1.188.1. RHSA-2010:0237: Low security and bug fix update

Updated sendmail packages that fix two security issues and several bugs are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having low security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

Sendmail is a very widely used Mail Transport Agent (MTA). MTAs deliver mail from one machine to another. Sendmail is not a client program, but rather a behind-the-scenes daemon that moves email over networks or the Internet to its final destination.

The configuration of sendmail in Red Hat Enterprise Linux was found to not reject the "localhost.localdomain" domain name for email messages that come from external hosts. This could allow remote attackers to disguise spoofed messages. ([CVE-2006-7176](#)<sup>1952</sup>)

A flaw was found in the way sendmail handled NUL characters in the CommonName field of X.509 certificates. An attacker able to get a carefully-crafted certificate signed by a trusted Certificate Authority could trick sendmail into accepting it by mistake, allowing the attacker to perform a man-in-the-middle attack or bypass intended client certificate authentication. ([CVE-2009-4565](#)<sup>1953</sup>)

Note: The [CVE-2009-4565](#)<sup>1954</sup> issue only affected configurations using TLS with certificate verification and CommonName checking enabled, which is not a typical configuration.

This update also fixes the following bugs:

---

<sup>1952</sup> <https://www.redhat.com/security/data/cve/CVE-2006-7176.html>

<sup>1953</sup> <https://www.redhat.com/security/data/cve/CVE-2009-4565.html>

<sup>1954</sup> <https://www.redhat.com/security/data/cve/CVE-2009-4565.html>

- \* sendmail was unable to parse files specified by the ServiceSwitchFile option which used a colon as a separator. ([BZ#512871](#)<sup>1955</sup>)
- \* sendmail incorrectly returned a zero exit code when free space was low. ([BZ#299951](#)<sup>1956</sup>)
- \* the sendmail manual page had a blank space between the -qG option and parameter. ([BZ#250552](#)<sup>1957</sup>)
- \* the comments in the sendmail.mc file specified the wrong path to SSL certificates. ([BZ#244012](#)<sup>1958</sup>)
- \* the sendmail packages did not provide the MTA capability. ([BZ#494408](#)<sup>1959</sup>)

All users of sendmail are advised to upgrade to these updated packages, which resolve these issues.

## 1.189. shadow-utils

### 1.189.1. RHBA-2010:0209: bug fix update

An updated shadow-utils package that fixes several bugs is now available.

The shadow-utils package includes programs for converting UNIX password files to the shadow password format, as well as tools for managing user and group accounts.

The updated shadow-utils package fixes the following bugs:

- \* shadow-utils package updates would overwrite the /etc/default/useradd directory. This would cause site configuration settings to be lost. Updates no longer overwrite the /etc/default/useradd directory, and site configuration changes are maintained. ([BZ#510102](#)<sup>1960</sup>)
- \* the newusers utility allows a batch of new users to be created and updated. The utility was not checking the range of generated UIDs (user identifiers) or GIDs (group identifiers). When used on AMD64 and Intel 64 systems, identifiers could be negative numbers outside the valid range of 500 to 60,000. The newusers utility now checks the range of generated UIDs and GIDs so that they do not appear outside the valid range. ([BZ#306241](#)<sup>1961</sup>)
- \* the newusers utility failed if a specified parent directory did not exist. The error message, 'mkdir failed', did not detail the cause of the failure. The newusers utility has been updated to note when the parent directory does not exist, and the manual page now emphasizes how non-existent parent directories are dealt with. The behavior of the newusers utility in this situation is now clearer. ([BZ#461455](#)<sup>1962</sup>)
- \* the useradd utility is used to create or update a new user's default information. The useradd utility did not recognize the base directory option (-b, --base-dir), and commands using this option would not succeed. The useradd utility has been updated to recognize the base directory option properly, and useradd commands now work as expected. ([BZ#469158](#)<sup>1963</sup>)

---

<sup>1955</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=512871](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=512871)

<sup>1956</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=299951](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=299951)

<sup>1957</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=250552](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=250552)

<sup>1958</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=244012](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=244012)

<sup>1959</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=494408](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=494408)

<sup>1960</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=510102](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=510102)

<sup>1961</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=306241](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=306241)

<sup>1962</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=461455](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=461455)

<sup>1963</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=469158](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=469158)

- \* the `useradd` utility did not reset the error number variable before checking function return values. As a consequence, error numbers could be affected by retained values, and the utility would fail with 'invalid numeric argument'. The error number variable is now reset before each function call, and error numbers in the `useradd` utility are reported correctly. ([BZ#487575](https://bugzilla.redhat.com/show_bug.cgi?id=487575)<sup>1964</sup>)
- \* the `useradd` utility handled the creation of UIDs differently on x86 and PowerPC 64 architectures than it did on others. As a consequence, UIDs greater than 2147483647 were rejected on these systems. The `useradd` utility now treats UIDs the same across architectures, and large UIDs are not rejected on x86 and PowerPC 64 architectures. ([BZ#505033](https://bugzilla.redhat.com/show_bug.cgi?id=505033)<sup>1965</sup>)
- \* the `usermod` utility allows a user account to be modified. The `usermod` utility did not support LDAP (Lightweight Directory Access Protocol) users, despite support in other utilities. As a result, the `usermod` utility could not add LDAP users to local groups. LDAP support has now been added to the `usermod` utility, and LDAP users can be added to local groups. ([BZ#449154](https://bugzilla.redhat.com/show_bug.cgi?id=449154)<sup>1966</sup>)
- \* the `restorecon` command sets file security contexts. The `usermod` utility was calling the `restorecon` command every time a user's home directory was changed. This would result in an error if expected files no longer existed. The `restorecon` command is no longer called by the `usermod` utility, and changing a user's home directory succeeds as expected. ([BZ#494575](https://bugzilla.redhat.com/show_bug.cgi?id=494575)<sup>1967</sup>)
- \* the `faillog` utility displays failure logs and sets login failure limits. When the utility was used with the print option (-p), the log was read sequentially to print in UID order. This was unnecessary and caused long print times. The `faillog` utility has been updated to print without ordering, and printing now completes in an acceptable time. ([BZ#473054](https://bugzilla.redhat.com/show_bug.cgi?id=473054)<sup>1968</sup>)
- \* the `grpconv` utility converts shadow passwords and groups. The utility was not checking whether duplicate group entries existed in the `/etc/group` directory. Running the utility with duplicate entries would consume too much memory. The `grpconv` utility now checks for duplicate group entries in the `/etc/group` directory, and excess memory is no longer consumed. ([BZ#507706](https://bugzilla.redhat.com/show_bug.cgi?id=507706)<sup>1969</sup>)

All users of shadow-utils are advised to upgrade to this updated package, which resolves these issues.

## 1.190. sosreport

### 1.190.1. RHBA-2010:0201: bug fix and enhancement update

**SOS** is a set of tools that gathers information about system hardware and configuration. The information can then be used for diagnostic purposes and debugging. **SOS** is commonly used to help support technicians and developers.

This update includes the following fixes:

- when `kmod-gfs2` was installed on a Red Hat Enterprise Linux 5 system, it was possible to have a situation whereby its version of `gfs2.ko` would take precedence over that supplied with the kernel. As a consequence, the wrong version of the **Global File System** would be used and it also would be incorrectly set to *weak-update*. **SOS** has now been modified to warn system administrators if

---

<sup>1964</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=487575](https://bugzilla.redhat.com/show_bug.cgi?id=487575)

<sup>1965</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=505033](https://bugzilla.redhat.com/show_bug.cgi?id=505033)

<sup>1966</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=449154](https://bugzilla.redhat.com/show_bug.cgi?id=449154)

<sup>1967</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=494575](https://bugzilla.redhat.com/show_bug.cgi?id=494575)

<sup>1968</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=473054](https://bugzilla.redhat.com/show_bug.cgi?id=473054)

<sup>1969</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=507706](https://bugzilla.redhat.com/show_bug.cgi?id=507706)

- gfs2.ko** has been set to use weak updates and instructs them there is a need to remove `kmmod-gfs2` and reboot the system before proceeding any further. ([BZ#507390](#)<sup>1970</sup>)
- **groupd** can erroneously assign the fence domain id 00000000. This can result in **LVM** commands becoming permanently locked. To alert system administrators to this issue, a check has been added to **SOS** that examines the output of `group_tool -v` for a string of zeroes against fence and, if it finds this to be the case, it generates a warning message that instructs administrators on how to remedy the problem. ([BZ#499468](#)<sup>1971</sup>)
  - **SOS** was inadvertently copying all subdirectories and files relative to where the command was executed, (including paths created by symlinks), into `/tmp`. (This problem did not occur if absolute link entries were used.) A change has been made so that **SOS** no longer traverses directories relative to the current working directory. As a result, this potentially large amount of data is no longer copied erroneously. ([BZ#530385](#)<sup>1972</sup>)
  - **SOS** had no capability to detect or report problems with cman services, which can occur when **groupd** becomes stuck in a state that needs to be resolved before cluster operations can continue. To rectify this, **SOS** now checks the output of `group_tool -v` to detect if **CMAN** services are set to anything other than *none*. A warning is then produced to prompt the system administrator to investigate the cause of the potential problem. ([BZ#499472](#)<sup>1973</sup>)
  - **SOS's** progress reporting was inaccurate, due to problems with output buffering and the wrong placement of error messages. When the `sosreport` command was run from a terminal, the percentage completed figure would go up and down. Furthermore, after it has reached 100%, the real time and estimated finish time would continue to grow together for several more seconds. A new, more reliable progress indication system has been added. As a result, the progress indication will be reliable from now on. ([BZ#502442](#)<sup>1974</sup>)
  - **SOS** would erroneously report that *one or more nfs export do not have a fsid attribute set* even if the `fsid` had been specified in the fs resource. This was due to an omission in the `cluster.py` file which was only searching the services tag and not the resources tag, in which `fsid` is set (as part of best practice) if the file system is a share resource. `cluster.py` has now been patched to account for all scenarios so false reports of missing `fsids` will no longer be generated. ([BZ#507674](#)<sup>1975</sup>)
  - The `sosreport -k general.syslogsize=15` command did not limit log file sizes to 15 Mb, contrary to expected behavior. This was because the limits were being erroneously applied to `/var/log/messages.*` instead of `/var/log/messages`. As a result, huge reports were generated and `sosreport` could even potentially die if all space in `/tmp` was used by the process. To fix this problem, the limits are now being applied to `/var/log/messages` meaning the huge reports are no longer being generated. ([BZ#516551](#)<sup>1976</sup>)
  - The list of installed RPMs generated by `sosreport` was in a non-standard format. Rather than in the accepted format of `name-[epoch:]version-release.arch`, it was in the form of `name-version-release.arch`. This was inconvenient to users wishing to paste output to programs such as `yum`. To fix this issue, changes have been made to ensure that the list of installed RPMs is now in the `name-[epoch:]version-release.arch` format to make it usable with `yum` and `rpm` commands. ([BZ#482755](#)<sup>1977</sup>)
  - A problem occurred when `sosreport` deliberately obscured fencing passwords in `/etc/cluster/cluster.conf`. It would break the XML formatting by removing the quotation marks that surrounded the masked version of the password. A further problem was that the passwords in backup files (such as `/etc/cluster/cluster.conf.1`) were not obscured. To resolve this



issue, changes have been made to password masking to ensure the XML remains well-formed and the process is applied to any back-up configuration files that may exist. As a result, security is enhanced and files no longer need manual rectification before tests can be run on `cluster.conf`. ([BZ#497588](#)<sup>1978</sup>)

- **SOS** reports were including all of the contents of the `/tftpboot` directory, which resulted in huge files (potentially greater than 1 GB), if multiple boot media had been created in that location. To address this issue the contents of `/tftpboot` are now excluded from the report. ([BZ#523263](#)<sup>1979</sup>)
- previously, the `sar` plugin included in **SOS** ignored the locale setting and created sar files with time data presented in the default format. With this update, the plugin now honors the locale setting and generates sar files with time data in the expected format (ie the same format as sar files created by `sysstat cron` jobs). ([BZ#525010](#)<sup>1980</sup>)

This update also adds the following enhancements:

- SOS was only gathering limited data on some aspects of system performance. This has been expanded to include sources such as:

```
/var/log/cron*
parted hard disk device print
tune2fs -l filesystem
/etc/inittab
service service name status
/etc/inittab
/etc/kdump.conf
/sbin/mdadm -D /dev/md*
/etc/lvm
/proc/buddyinfo
```

As a result, a much broader variety of reports are displayed for a number of different aspects of the system, making troubleshooting easier. ([BZ#453151](#)<sup>1981</sup>, [BZ#517028](#)<sup>1982</sup>, [BZ#429398](#)<sup>1983</sup>)

- SOS was not gathering dmraid information, which can be extremely useful for troubleshooting. A large amount of functionality has now been added that enables SOS to report dm-raid signatures if these are detected and send this information to support engineers. It also ensures that this information is reported even if SOS is being run in rescue mood at one of the service levels at which dm-raid systems will not boot. This information is gathered via these specific commands:

```
dmraid -V
dmraid -b
dmraid -r
dmraid -s
dmraid -tay
dmraid -rD
```

the output of which is now gathered by `sosreport` resulting in much quicker identification and resolution of support issues. ([BZ#507672](#)<sup>1984</sup>)

- SOS was not reporting configuration information for running OpenAIS systems, making troubleshooting extremely difficult, especially if the systems in question had been heavily customized. SOS has been modified so that the following detailed OpenAIS cluster information is now captured, leading to faster and more accurate troubleshooting. ([BZ#521344](#)<sup>1985</sup>)



- the rh-upload-core script included with sos has been improved. Most significantly, the script can now upload any file, and not just vmcores. ([BZ#523750](#)<sup>1986</sup>)
- SOS reports include the name service cache daemon (nscd) configuration file found at /etc/nscd.conf. With this update, SOS reports now also include the debug logs if nscd is running with debugging enabled. Note: similarly to syslog, SOS limits the debug log files to 50 MiB. If nscd runs in debug mode for extended periods (eg a week), the debug log files can be 100s of MiBs and larger. ([BZ#536960](#)<sup>1987</sup>)
- SOS now checks for the presence of Apache QPID (specifically, it checks for qpidd, the QPID daemon) and, if detected, collects QPID configuration, state and log information and saves it to sos\_command/broker/ in the sosreport. ([BZ#557851](#)<sup>1988</sup>)
- SOS did not gather the SELinux audit log files (/var/log/audit/\*). It has now been amended to gather the last fifty entries of this log, meaning that SELinux problems can be investigated more easily. ([BZ#443984](#)<sup>1989</sup>)
- SOS did not gather sound card information, leading to prolonged support calls whilst this information was manually collected and sent in by users. A new Python-based plug-in has been written that collects information about soundcards via ALSA. As a result, users will not have to hunt for this information themselves during a support call. ([BZ#478009](#)<sup>1990</sup>)
- SOS was not reporting the output of the lsb\_release command. If /etc/redhat-release was corrupted or missing, it was impossible for support to confirm which version of Red Hat Enterprise Linux was in use. lsb\_release provides a useful fallback. A plug-in has been added to SOS to gather a large amount of data provided by the lsb\_release command and in associated /etc files. It also outputs a message, informing the user if /etc/redhat-release is missing. By reporting this information, the system version can be identified quickly and accurately, assisting in the troubleshooting process. ([BZ#479111](#)<sup>1991</sup>)
- SOS was not able to collect data relating to the Quagga routing suite if this was installed on a user's systems. As a result, troubleshooting these systems was more difficult. To remedy this problem, a plug-in has been added to SOS that collects Quagga-related configuration files, thereby providing the requisite information to quickly and easily identify and remedy problems with these systems. ([BZ#485191](#)<sup>1992</sup>)
- SOS was not able to collect Cron data. As a result, troubleshooting was sometimes difficult. To resolve this issue, SOS has been patched so that it now includes data from /var/spool/cron allowing support engineers to know about the scheduling of tasks on a given system. ([BZ#485559](#)<sup>1993</sup>)
- SOS was not able to report information about the Cobbler Linux installation suite, limiting engineers' attempts to troubleshoot systems. To rectify this, SOS now has a plug-in that gathers the following files if they are present:

```
/etc/cobbler
/var/log/cobbler
/var/lib/rhn/kickstarts
/var/lib/cobbler/snippets
/var/lib/cobbler/config
/var/lib/cobbler/kickstarts
/var/lib/cobbler/triggers
```

As a result, troubleshooting Cobbler is now much easier. ([BZ#495934](#)<sup>1994</sup>).

- SOS was not able to report information about the iSCSI Initiator if this was present on the system. Thus, information about transmission of SCSI commands over IP networks could not be gathered by the reporting tool. To rectify this problem, SOS now reports on:

```
/etc/iscsi/iscsid.conf
/etc/iscsi/initiatorname.iscsi
/var/lib/iscsi/
```

This makes debugging problems involving iSCSI much easier. ([BZ#512889](#)<sup>1995</sup>)

- SOS was not able to capture multicast information This made it hard to debug OpenAIS clusters, as they use multicast IGMP groups to send messages. For the purposes of troubleshooting, it is important to know which groups are available and active on a node, so SOS has been enhanced so that it can now report on the following information:

```
netstat -agn
ip mroute show
ip maddr show
```

As a result, OpenAIS clusters can now be debugged by troubleshooters much more easily. ([BZ#514294](#)<sup>1996</sup>)

All sosreport users should install this updated package, which addresses these issues and adds these enhancements.

## 1.191. squid

### 1.191.1. RHSA-2010:0221: Low security and bug fix update

An updated squid package that fixes two security issues and several bugs is now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having low security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

Squid is a high-performance proxy caching server for web clients, supporting FTP, Gopher, and HTTP data objects.

A flaw was found in the way Squid processed certain external ACL helper HTTP header fields that contained a delimiter that was not a comma. A remote attacker could issue a crafted request to the Squid server, causing excessive CPU use (up to 100%). ([CVE-2009-2855](#)<sup>1997</sup>)

Note: The [CVE-2009-2855](#)<sup>1998</sup> issue only affected non-default configurations that use an external ACL helper script.

A flaw was found in the way Squid handled truncated DNS replies. A remote attacker able to send specially-crafted UDP packets to Squid's DNS client port could trigger an assertion failure in Squid's child process, causing that child process to exit. ([CVE-2010-0308](#)<sup>1999</sup>)

---

<sup>1997</sup> <https://www.redhat.com/security/data/cve/CVE-2009-2855.html>

<sup>1998</sup> <https://www.redhat.com/security/data/cve/CVE-2009-2855.html>

<sup>1999</sup> <https://www.redhat.com/security/data/cve/CVE-2010-0308.html>

This update also fixes the following bugs:

\* Squid's init script returns a non-zero value when trying to stop a stopped service. This is not LSB compliant and can generate difficulties in cluster environments. This update makes stopping LSB compliant. ([BZ#521926](https://bugzilla.redhat.com/show_bug.cgi?id=521926)<sup>2000</sup>)

\* Squid is not currently built to support MAC address filtering in ACLs. This update includes support for MAC address filtering. ([BZ#496170](https://bugzilla.redhat.com/show_bug.cgi?id=496170)<sup>2001</sup>)

\* Squid is not currently built to support Kerberos negotiate authentication. This update enables Kerberos authentication. ([BZ#516245](https://bugzilla.redhat.com/show_bug.cgi?id=516245)<sup>2002</sup>)

\* Squid does not include the port number as part of URIs it constructs when configured as an accelerator. This results in a 403 error. This update corrects this behavior. ([BZ#538738](https://bugzilla.redhat.com/show_bug.cgi?id=538738)<sup>2003</sup>)

\* the `error_map` feature does not work if the same handling is set also on the HTTP server that operates in deflate mode. This update fixes this issue. ([BZ#470843](https://bugzilla.redhat.com/show_bug.cgi?id=470843)<sup>2004</sup>)

All users of squid should upgrade to this updated package, which resolves these issues. After installing this update, the squid service will be restarted automatically.

## 1.192. squirrelmail

### 1.192.1. RHSA-2009:1490: Moderate security update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2009:1490](https://www.redhat.com/security/data/cve/RHSA-2009:1490)<sup>2005</sup>

An updated squirrelmail package that fixes several security issues is now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

SquirrelMail is a standards-based webmail package written in PHP.

Form submissions in SquirrelMail did not implement protection against Cross-Site Request Forgery (CSRF) attacks. If a remote attacker tricked a user into visiting a malicious web page, the attacker could hijack that user's authentication, inject malicious content into that user's preferences, or possibly send mail without that user's permission. ([CVE-2009-2964](https://www.redhat.com/security/data/cve/CVE-2009-2964)<sup>2006</sup>)

Users of SquirrelMail should upgrade to this updated package, which contains a backported patch to correct these issues.

<sup>2000</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=521926](https://bugzilla.redhat.com/show_bug.cgi?id=521926)

<sup>2001</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=496170](https://bugzilla.redhat.com/show_bug.cgi?id=496170)

<sup>2002</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=516245](https://bugzilla.redhat.com/show_bug.cgi?id=516245)

<sup>2003</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=538738](https://bugzilla.redhat.com/show_bug.cgi?id=538738)

<sup>2004</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=470843](https://bugzilla.redhat.com/show_bug.cgi?id=470843)

<sup>2006</sup> <https://www.redhat.com/security/data/cve/CVE-2009-2964.html>

## 1.193. star

### 1.193.1. RHBA-2009:1575: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTRACK errata [RHBA-2009:1575](#)<sup>2007</sup>

An updated star package that fixes a bug is now available.

The star utility is a tape- and disk-archiving tool similar to tar that supports saving Access Control List (ACLs) permission information.

This updated star package fixes the following bug:

\* restoring directories which had default ACL permissions set when they were archived with the star utility did not result in those ACL permissions correctly being restored after extraction. This update fixes the problem so that the default ACL permissions are correctly restored on directories extracted from a star archive. ([BZ#450994](#)<sup>2008</sup>)

All users of star are advised to upgrade to this updated package, which resolves this issue.

## 1.194. strace

### 1.194.1. RHBA-2010:0047: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2010:0047](#)<sup>2009</sup>

An updated strace package that fixes a bug when tracing a program that blocks the SIGTRAP signal is now available.

The strace program intercepts and records the system calls called and received by a running process. Strace can print a record of each system call, its arguments and its return value.

This updated strace package fixes the following bug:

\* the kernel does not send SIGTRAP notifications to strace after an execve system call finishes. Consequently, when "strace -f" was executed against a program that blocked the SIGTRAP signal and subsequently called execve, strace sent a "[preattached child 0 of 12166 in weird state!]" message to STD OUT and hung. With this update, strace now checks for this situation and re-synchronizes with system call notifications when necessary. Note: this problem only presents on Itanium-based systems ([BZ#548363](#)<sup>2010</sup>)

All strace users are advised to upgrade to this updated package, which resolves this issue.

---

<sup>2008</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=450994](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=450994)

<sup>2010</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=548363](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=548363)

## 1.194.2. RHBA-2010:0174: bug fix update



### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2010:0174](#)<sup>2011</sup>

An updated strace package that fixes two bugs is now available.

The strace program intercepts and records the system calls called and received by a running process. Strace can print a record of each system call, its arguments and its return value.

This updated strace package fixes the following bugs:

\* when an strace process was terminated by a signal while the tracee was executing a fork or clone system call the tracee was forcefully terminated instead of being cleanly detached. This update corrects this: tracees are now cleanly detached as expected when an strace process is terminated in the circumstance noted above. ([BZ#558471](#)<sup>2012</sup>)

\* RHBA-2010:0047, the strace update released to address [BZ#548363](#)<sup>2013</sup>, uncovered a race condition on Itanium-based systems. (See References below for a link to this previous release.) The race condition presented when strace attached to a process while said process was executing the execve system call. With this update, strace now reliably detects this post-execve trap and, consequently, avoids the race condition. ([BZ#564364](#)<sup>2014</sup>)

## 1.195. sudo

### 1.195.1. RHSA-2010:0122: Important security update



### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2010:0122](#)<sup>2015</sup>

An updated sudo package that fixes two security issues is now available for Red Hat Enterprise Linux 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

The sudo (superuser do) utility allows system administrators to give certain users the ability to run commands as root.

A privilege escalation flaw was found in the way sudo handled the sudoedit pseudo-command. If a local user were authorized by the sudoers file to use this pseudo-command, they could possibly leverage this flaw to execute arbitrary code with the privileges of the root user. ([CVE-2010-0426](#)<sup>2016</sup>)

<sup>2012</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=558471](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=558471)

<sup>2013</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=548363](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=548363)

<sup>2014</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=564364](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=564364)

<sup>2016</sup> <https://www.redhat.com/security/data/cve/CVE-2010-0426.html>

The sudo utility did not properly initialize supplementary groups when the "runas\_default" option (in the sudoers file) was used. If a local user were authorized by the sudoers file to perform their sudo commands under the account specified with "runas\_default", they would receive the root user's supplementary groups instead of those of the intended target user, giving them unintended privileges. ([CVE-2010-0427](https://www.redhat.com/security/data/cve/CVE-2010-0427.html)<sup>2017</sup>)

Users of sudo should upgrade to this updated package, which contains backported patches to correct these issues.

### 1.195.2. RHBA-2010:0212: bug fix update

An updated sudo package that fixes various bugs is now available.

The sudo (super user do) utility allows system administrators to give certain users the ability to run commands as root with logging.

This update addresses the following issues:

- \* if `runas_default=[value]` was set in the sudoers file, running a command such as "sudo -i" returned a collection of system groups rather than switching the current user to the user specified by the `runas_default` parameter. This has been corrected with this update: setting the `runas_default` parameter in the sudoers file now works as expected. ([BZ#497873](https://bugzilla.redhat.com/show_bug.cgi?id=497873)<sup>2018</sup>)
- \* the `/etc/sudoers` configuration file supports expressing ranges such as "[A-Z]" and "[a-z]" when delineating permissions on files. However, the range "[A-z]" (uppercase 'A' to lowercase 'z') was not equivalent to "[A-Za-z]" in certain locales, such as those using the UTF-8 character encoding. With this update, the range "[A-z]" can be used in the sudoers file to restrict access to files with names that use only basic Latin alphabetical characters. ([BZ#512191](https://bugzilla.redhat.com/show_bug.cgi?id=512191)<sup>2019</sup>)
- \* the variable used for iterating wildcards (such as \* and !) was being freed incorrectly. As a consequence, situations where a single file with a long file name was the only wildcard match would result in an error, restricting access. The sudo utility now correctly frees the glob iterator, and long file names work as expected with wildcard characters. ([BZ#521778](https://bugzilla.redhat.com/show_bug.cgi?id=521778)<sup>2020</sup>)
- \* visudo is a tool for editing the sudoers file that locks against simultaneous editing and provides other error checking. The visudo tool did not support unused aliases, and as a result any unused aliases in the sudoers file would cause visudo to fail with an error. The visudo tool has been updated to handle unused aliases, and now no longer fails when encountering them in the sudoers file. ([BZ#550326](https://bugzilla.redhat.com/show_bug.cgi?id=550326)<sup>2021</sup>)
- \* user names that are identical to process UIDs (unique identifiers), such as 'proxy', are allowable. Previously, sudo erroneously rejected commands such as 'sudo su - proxy', interpreting the user name as the process UID, resulting in these super users being unable to authenticate. The sudo utility now differentiates between user names and process UIDs, and users authenticate as expected. ([BZ#500942](https://bugzilla.redhat.com/show_bug.cgi?id=500942)<sup>2022</sup>)
- \* the `requiretty` option requires a user to use only a real terminal (TTY). When sudo was used over LDAP (Lightweight Directory Access Protocol), the `!requiretty` (TTY not required) option was incorrectly

---

<sup>2017</sup> <https://www.redhat.com/security/data/cve/CVE-2010-0427.html>

<sup>2018</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=497873](https://bugzilla.redhat.com/show_bug.cgi?id=497873)

<sup>2019</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=512191](https://bugzilla.redhat.com/show_bug.cgi?id=512191)

<sup>2020</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=521778](https://bugzilla.redhat.com/show_bug.cgi?id=521778)

<sup>2021</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=550326](https://bugzilla.redhat.com/show_bug.cgi?id=550326)

<sup>2022</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=](https://bugzilla.redhat.com/show_bug.cgi?id=)

interpreted, and access was not granted to users from non-TTY connections. The sudo utility now correctly sets the `!requiretty` option for LDAP users, and they can connect normally. ([BZ#521903](https://bugzilla.redhat.com/show_bug.cgi?id=521903)<sup>2023</sup>)

\* the `#includedir` directive includes the contents of external directories in the current file. The directive was not supported in the sudoers file and sudo utility, and as a result external settings files could not be included. The sudo utility now supports the `#includedir` directory, and external settings files can be used in the sudoers file. ([BZ#538700](https://bugzilla.redhat.com/show_bug.cgi?id=538700)<sup>2024</sup>)

\* a bug in the `realloc()` function caused sudo to crash with a segfault when using a sudoers file with a deep `#include` structure. This update corrects this. Note: the hard limit of 128 nested include files (enforced to prevent `#include` file loops) remains. ([BZ#561336](https://bugzilla.redhat.com/show_bug.cgi?id=561336)<sup>2025</sup>)

All users of sudo are advised to upgrade to this updated package, which resolves these issues.

## 1.196. sysklogd

### 1.196.1. RHBA-2010:0211: bug fix update

An updated sysklogd package that fixes various bugs is now available.

The sysklogd package contains two system utilities (`syslogd` and `klogd`) which provide support for system logging. `Syslogd` and `klogd` run as daemons (background processes) and log system messages to different places, like sendmail logs, security logs, error logs, etc.

This update addresses the following issues:

\* the Red Hat Enterprise Linux `syslogd` init script creates files which are readable by the root user only whereas the `sysklogd(8)` man page indicated that "If a file is created it is world readable". The man page has been updated with the correct information. ([BZ#460232](https://bugzilla.redhat.com/show_bug.cgi?id=460232)<sup>2026</sup>)

\* the `-S` option was added to `sysklogd` 1.4.1-40, however, this option is not displayed in the "SYNOPSIS" section of the `sysklogd` man page. This has the potential to mislead users who use the man page for help. The `-S` option has now been added to the "SYNOPSIS" section of the `sysklogd` man page. ([BZ#471174](https://bugzilla.redhat.com/show_bug.cgi?id=471174)<sup>2027</sup>)

\* when `syslogd` was started using the `-m` option with a non-zero argument, the `errno` value of "select" was checked by the functions that log the "MARK" message after the value had been reset from "EINTR" to "EINVAL". This resulted in an incorrect message being logged to `/var/log/messages` of the form; "syslogd: select: Invalid argument". A patch has been applied to store the value of `errno` in a temporary variable prior to it being reset and testing this stored value against "EINTR" for logging purposes. The error message no longer appears in `/var/log/messages` when a non-zero argument is passed to the `-m` option. ([BZ#472875](https://bugzilla.redhat.com/show_bug.cgi?id=472875)<sup>2028</sup>)

\* `syslogd.conf` would cause a memory leak by forwarding messages to its IP address, for example `*.*@192.168.122.5`. This would result in processes being terminated by the "OOM killer" to free up memory. A patch has been applied to ensure that messages are not self-forwarded. ([BZ#481600](https://bugzilla.redhat.com/show_bug.cgi?id=481600)<sup>2029</sup>)

<sup>2023</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=521903](https://bugzilla.redhat.com/show_bug.cgi?id=521903)

<sup>2024</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=538700](https://bugzilla.redhat.com/show_bug.cgi?id=538700)

<sup>2025</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=561336](https://bugzilla.redhat.com/show_bug.cgi?id=561336)

<sup>2026</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=460232](https://bugzilla.redhat.com/show_bug.cgi?id=460232)

<sup>2027</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=471174](https://bugzilla.redhat.com/show_bug.cgi?id=471174)

<sup>2028</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=472875](https://bugzilla.redhat.com/show_bug.cgi?id=472875)

<sup>2029</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=481600](https://bugzilla.redhat.com/show_bug.cgi?id=481600)



\* when syslog messages were logged to the console, line feeds were not inserted resulting in all messages being displayed on a single line. A patch has been applied to ensure that each message appears on a new line. ([BZ#490897](https://bugzilla.redhat.com/show_bug.cgi?id=490897)<sup>2030</sup>)

\* if the "SIGALRM" signal was triggered during processing of the "writeev()" function, syslog would cease logging to the console and print a "/dev/console: Interrupted system call" message. Additionally, log messages were truncated in the event that the I/O buffer became full. A patch has been applied to reschedule the "SIGALRM" signal prior to calling the "writeev()" function to ensure messages are correctly displayed to the console. ([BZ#506683](https://bugzilla.redhat.com/show_bug.cgi?id=506683)<sup>2031</sup>)

Users of sysklogd should upgrade to this updated package, which resolves these issues.

## 1.197. system-config-cluster

### 1.197.1. RHBA-2010:0288: bug fix update

An updated system-config-cluster package that fixes several bugs is now available.

The system-config-cluster package contains a utility that allows management of cluster configuration in a graphical setting.

This update fixes the following bugs:

\* underscores in node names are accidentally trimmed in cluster.conf://failoverdomainnode/@name ([BZ#352631](https://bugzilla.redhat.com/show_bug.cgi?id=352631)<sup>2032</sup>)

\* system-config-cluster says fence\_apc's "switch" option must be provided, but it's optional. ([BZ#436939](https://bugzilla.redhat.com/show_bug.cgi?id=436939)<sup>2033</sup>)

\* system-config-cluster and poorly formed xml error for vm resource. ([BZ#474155](https://bugzilla.redhat.com/show_bug.cgi?id=474155)<sup>2034</sup>)

\* system-config-cluster xml errors with \_independent\_subtree. ([BZ#476260](https://bugzilla.redhat.com/show_bug.cgi?id=476260)<sup>2035</sup>)

\* system-config-cluster parses glade widget values incorrectly. ([BZ#493996](https://bugzilla.redhat.com/show_bug.cgi?id=493996)<sup>2036</sup>)

\* system-config-cluster failed to create proper cluster.conf entries for gfs2 filesystem type. ([BZ#515443](https://bugzilla.redhat.com/show_bug.cgi?id=515443)<sup>2037</sup>)

\* system-config-cluster should not tag clusternodes with multicast tags. ([BZ#517140](https://bugzilla.redhat.com/show_bug.cgi?id=517140)<sup>2038</sup>)

\* system-config-cluster does not validate "startup\_wait" mysql resource option. ([BZ#530171](https://bugzilla.redhat.com/show_bug.cgi?id=530171)<sup>2039</sup>)

System-config-cluster users should upgrade to this updated package, which resolves these issues.

---

<sup>2030</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=490897](https://bugzilla.redhat.com/show_bug.cgi?id=490897)

<sup>2031</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=506683](https://bugzilla.redhat.com/show_bug.cgi?id=506683)

<sup>2032</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=352631](https://bugzilla.redhat.com/show_bug.cgi?id=352631)

<sup>2033</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=436939](https://bugzilla.redhat.com/show_bug.cgi?id=436939)

<sup>2034</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=474155](https://bugzilla.redhat.com/show_bug.cgi?id=474155)

<sup>2035</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=476260](https://bugzilla.redhat.com/show_bug.cgi?id=476260)

<sup>2036</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=493996](https://bugzilla.redhat.com/show_bug.cgi?id=493996)

<sup>2037</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=515443](https://bugzilla.redhat.com/show_bug.cgi?id=515443)

<sup>2038</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=517140](https://bugzilla.redhat.com/show_bug.cgi?id=517140)

<sup>2039</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=530171](https://bugzilla.redhat.com/show_bug.cgi?id=530171)

## 1.198. system-config-lvm

### 1.198.1. RHBA-2009:1613: bug-fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1613](#)<sup>2040</sup>

An updated system-config-lvm package that fixes a bug is now available.

The system-config-lvm package contains a utility for configuring logical volumes via a graphical user interface.

This updated package fixes the following bug:

\* in several non-English locales, clicking the Create New Logical Volume button in the Logical Volume Management GUI (system-config-lvm) caused a python error and did not present a Create New Logical Volume window as expected. This made it impossible to use system-config-lvm to create new logical volumes.

The Create New Logical Volume window includes a Filesystem combo box pop-up menu which has 'None' selected and displayed by default. The error above occurred on systems set to any locale which required non-ASCII characters to present the translated equivalent of the English 'None'. This includes locales such as Japanese (where the problem was reported in the field), Serbian and Slovak. With this update, the combo box pop-up menu has been corrected to enable the display of any UTF-8 character. In the affected locales the Create New Logical Volume window now appears and works as expected. ([BZ#537022](#)<sup>2041</sup>)

All system-config-lvm users are advised to upgrade to this updated package, which resolves this issue.

### 1.198.2. RHBA-2010:0267: bug fix update

Updated system-config-lvm packages that fix several bugs are now available.

system-config-lvm is a utility for graphically configuring logical volumes.

This update includes the following fixes:

\* system-config-lvm started very slowly. In these updated packages, system-config-lvm uses caching for such information, which resolves this issue. ([BZ#525116](#)<sup>2042</sup>)

\* system-config-lvm did not start correctly in some cases when a physical volume was created on a logical volume. In these updated packages, system-config-lvm contains fixes for this situation. ([BZ#522200](#)<sup>2043</sup>)

\* system-config-lvm failed when scanning mirrored logical volume with corelog. In these updated package, system-config-lvm works correctly with such volumes. ([BZ#516609](#)<sup>2044</sup>)

<sup>2041</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=537022](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=537022)

<sup>2042</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=525116](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=525116)

<sup>2043</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=522200](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=522200)

<sup>2044</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=516609](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=516609)

- \* system-config-lvm failed to create volumes in a Japanese environment. In these updated package, system-config-lvm correctly translates strings from/to correct encoding. ([BZ#515322](#)<sup>2045</sup>)
- \* system-config-lvm corrupted data when used on a volume exported through iSCSI. In these updated packages, system-config-lvm refuses to work with volumes which are used if they are not mounted. ([BZ#514268](#)<sup>2046</sup>)
- \* system-config-lvm started extremely slowly when used over a slow network. In these updated package, the system-config-lvm progress bar is updated less frequently but is still fluent even on local displays. ([BZ#502042](#)<sup>2047</sup>)
- \* system-config-lvm lost mount attributes in /etc/fstab after a change of volumes. In these updated packages, system-config-lvm preserves all attributes from /etc/fstab. ([BZ#475434](#)<sup>2048</sup>, [BZ#455945](#)<sup>2049</sup>)
- \* system-config-lvm did not support ext4 file systems. In these updated packages, system-config-lvm supports ext4 file systems. ([BZ#444525](#)<sup>2050</sup>)
- \* system-config-lvm did not work correctly in the Oriya language when some numbers where written using their glyphs. In these updated packages, system-config-lvm uses Arabic numbers everywhere. ([BZ#243646](#)<sup>2051</sup>)
- \* system-config-lvm used extents as a default unit size for volumes. In these updated package, system-config-lvm uses MB, GB, or TB, depending on the size of volume. ([BZ#217752](#)<sup>2052</sup>)

Users are advised to upgrade to these updated system-config-lvm packages, which resolve these issues.

## 1.199. system-config-securitylevel

### 1.199.1. RHBA-2009:1656: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTRACK errata [RHBA-2009:1656](#)<sup>2053</sup>

Updated system-config-securitylevel packages that fix several bugs are now available.

system-config-securitylevel is a graphical program for configuring firewall and SELinux settings.

These updated packages address the following bugs:

- \* when a new port is added to a firewall -- via the Firewall Options > Other ports > Add dialog box -- its service name is derived from the port number. Service names containing hyphens (eg iascontrol-oms,

---

<sup>2045</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=515322](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=515322)

<sup>2046</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=514268](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=514268)

<sup>2047</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=502042](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=502042)

<sup>2048</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=475434](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=475434)

<sup>2049</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=455945](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=455945)

<sup>2050</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=444525](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=444525)

<sup>2051</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=243646](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=243646)

<sup>2052</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=217752](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=217752)

1156/TCP, the Oracle Application Server control port) were incorrectly assumed to be port ranges. This caused them to be split, with the individual sections found to be invalid. Note: this validation failure did not prevent the port from being added to the firewall, as could be seen with the iptables-save command. The port was not listed in the "Other ports" list, however. With this update service names with hyphens are treated correctly, the added port is validated correctly and it is listed in "Other ports" as expected. ([BZ#503588](#)<sup>2054</sup>)

\* system-config-securitylevel-tui, the text-based equivalent to system-config-securitylevel, relies on the setenforce command but did not have an explicit dependency on libselinux, the package that provides the setenforce command. With this update, the system-config-securitylevel spec file has been updated to require libselinux, ensuring system-config-securitylevel-tui always has the setenforce command available as needed. ([BZ#532947](#)<sup>2055</sup>)

\* lokkit calls referenced setenforce without explicitly noting its path: /usr/sbin/setenforce. The default PATH for ordinary users on Red Hat Enterprise Linux does not include /usr/sbin/, however. If such users had sudo-based permission to run system-config-securitylevel-tui, attempting to run this application resulted in a "sh: setenforce: command not found" error. lokkit now references setenforce's path explicitly and ordinary users with appropriate permissions can run system-config-securitylevel-tui as expected. Note: /usr/sbin is in the default PATH of the root user on Red Hat Enterprise Linux. If system-config-securitylevel-tui was only run by the root user, this error did not present. ([BZ#532948](#)<sup>2056</sup>)

All users are advised to upgrade to these updated packages, which resolve these issues.

## 1.200. system-config-services

### 1.200.1. RHBA-2010:0275: bug fix update

An updated system-config-services package that fixes several bugs is now available.

system-config-services is a utility which allows you to configure which services should be enabled on your machine.

This updated system-config-services package includes fixes for the following bugs:

\* as included in Red Hat Enterprise Linux 5, system-config-services has several new options that were not properly documented in the Help files available via the Help menu. These undocumented options include a "Runlevel All" option under "Edit RunLevel" and an "On Demand Services" tab. Updated documentation that covers these options has been written and added to the Help menu directory: /usr/share/doc/system-config-services-0.9.4/html/. ([BZ#208170](#)<sup>2057</sup>, [BZ#370461](#)<sup>2058</sup>)

\* po files used to populate the German-language version of the system-config-services user interface were not properly UTF-8 encoded: they contained incorrect characters that resulted in a nonsense strings presenting when the application was used in German. These characters have been corrected to their corresponding UTF-8 characters, ensuring they display properly in German locales. ([BZ#284931](#)<sup>2059</sup>)

---

<sup>2054</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=503588](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=503588)

<sup>2055</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=532947](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=532947)

<sup>2056</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=532948](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=532948)

<sup>2057</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=208170](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=208170)

<sup>2058</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=370461](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=370461)

<sup>2059</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=284931](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=284931)

\* After making changes to on-demand xinetd services, clicking "Restart" in the "Background Services" tab resulted in a traceback. This updated version restarts the selected background service as expected and correctly handles xinetd service changes. ([BZ#445185](https://bugzilla.redhat.com/show_bug.cgi?id=445185)<sup>2060</sup>)

\* if a non-existent service name was added (via the Actions > Add Service dialog box), system-config-services provided no user-level feedback of the error but did write a traceback error to the console. With this update, system-config-services presents an error alert box when a non-existent service is added and no longer produces a traceback error. This update also addresses an equivalent problem that occurred when deleting a disabled service via Actions > Delete Service. This action now works as expected. ([BZ#500424](https://bugzilla.redhat.com/show_bug.cgi?id=500424)<sup>2061</sup>)

All system-config-services users should install this updated package which addresses these issues.

## 1.201. systemtap

### 1.201.1. RHBA-2010:0070: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2010:0070](https://errata.redhat.com/RHBA-2010:0070)<sup>2062</sup>

Updated systemtap packages that fix a bug that could cause kernel panics are now available.

SystemTap is an instrumentation system for systems running the Linux kernel, version 2.6. Developers can write scripts to collect data on the operation of the system.

This update addresses the following issue:

\* abnormal shutdowns, triggered at the same time as probe startups, triggered a race condition, and consequent kernel panics, when multiple systemtap commands ran simultaneously. The probe setup could be called during or after the probe shutdown which lead to kernel callbacks remaining registered after modules were unloaded. Setup activities, shutdown activities and related flags are now guarded by mutex (mutual exclusion) algorithms, ensuring strict ordering which obviates the race condition and prevents the kernel panics from occurring. This update also includes a new test `-- /usr/share/systemtap/testsuite/systemtap.base/pr10854.exp --` that checks for this race condition. ([BZ#543058](https://bugzilla.redhat.com/show_bug.cgi?id=543058)<sup>2063</sup>)

All systemtap users should upgrade to these updated packages, which resolve this issue.

### 1.201.2. RHSA-2010:0124: Important security update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2010:0124](https://errata.redhat.com/RHSA-2010:0124)<sup>2064</sup>

---

<sup>2060</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=445185](https://bugzilla.redhat.com/show_bug.cgi?id=445185)

<sup>2061</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=500424](https://bugzilla.redhat.com/show_bug.cgi?id=500424)

<sup>2063</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=543058](https://bugzilla.redhat.com/show_bug.cgi?id=543058)

Updated systemtap packages that fix two security issues are now available for Red Hat Enterprise Linux 5.

This update has been rated as having important security impact by the Red Hat Security Response Team.

SystemTap is an instrumentation system for systems running the Linux kernel, version 2.6. Developers can write scripts to collect data on the operation of the system.

A flaw was found in the SystemTap compile server, `stap-server`, an optional component of SystemTap. This server did not adequately sanitize input provided by the `stap-client` program, which may allow a remote user to execute arbitrary shell code with the privileges of the compile server process, which could possibly be running as the root user. ([CVE-2009-4273](#)<sup>2065</sup>)

Note: `stap-server` is not run by default. It must be started by a user or administrator.

A buffer overflow flaw was found in SystemTap's `tapset __get_argv()` function. If a privileged user ran a SystemTap script that called this function, a local, unprivileged user could, while that script is still running, trigger this flaw and cause memory corruption by running a command with a large argument list, which may lead to a system crash or, potentially, arbitrary code execution with root privileges. ([CVE-2010-0411](#)<sup>2066</sup>)

Note: SystemTap scripts that call `__get_argv()`, being a privileged function, can only be executed by the root user or users in the `stapdev` group. As well, if such a script was compiled and installed by root, users in the `stapusr` group would also be able to execute it.

SystemTap users should upgrade to these updated packages, which contain backported patches to correct these issues.

### 1.201.3. RHBA-2010:0308: bug fix and enhancement update

SystemTap provides an instrumentation infrastructure for systems running the Linux 2.6 kernel. It allows users to write scripts that probe and trace system events for monitoring and profiling purposes. SystemTap's framework allows users to investigate and monitor a wide variety of kernel functions, system calls, and other events that occur in both kernel-space and user-space.

With this update, SystemTap is now re-based on upstream release version 1.1 ([BZ#515829](#)<sup>2067</sup>). This update also applies the following fixes and enhancements:

- The **systemtap-testsuite** package contained test cases that were incorrectly not configured as 'executable' (**systemtap.base/bz10078.stp**, **buildko/two.stp**, and **buildok/thirty.stp**). Any test runs involving these cases failed unexpectedly. This release fixes the permissions for all test cases; it also fixes minor test case issues relating to an incorrect header file reference in **systemtap.base/sdt.exp**, an incorrect execution sequence in **systemtap.base/labels.exp**, and an incorrect reference to a missing script in **systemtap.base/crash.exp**. ([BZ#506959](#)<sup>2068</sup>, [BZ#559643](#)<sup>2069</sup>, and [BZ#513654](#)<sup>2070</sup>)
- This update also fixes several typographical errors in the **man** pages of **stap-server** and **stap-client**. ([BZ#516691](#)<sup>2071</sup>)

<sup>2065</sup> <https://www.redhat.com/security/data/cve/CVE-2009-4273.html>

<sup>2066</sup> <https://www.redhat.com/security/data/cve/CVE-2010-0411.html>

<sup>2067</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=515829](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=515829)

- Using the `task_pid()` function in a SystemTap script while the `kernel-debuginfo` package was not installed could incorrectly result in a semantic error. This update applies an upstream patch to the `task.stp` tapset, which fixes the issue. ([BZ#519314](#)<sup>2072</sup>)
- This release also includes sample scripts for probing kernel tracepoints, namely:
  - `memory/mmanonpage.stp`
  - `memory/mmfilepage.stp`
  - `memory/mmreclaim.stp`
  - `memory/mmwriteback.stp`
  - `network/dropwatch.stp`
  - `process/schedtimes.stp`([BZ#497894](#)<sup>2073</sup>)
- Killing concurrent `staprun` processes could result in a kernel panic. This was because `runtime/procfs.c` only checked if `/proc/systemtap` was being used before deleting it, resulting in a race condition that made it possible for `/proc/systemtap` to be deleted while a module was still loaded inside. This update fixes the race condition by adding instructions to lock the transport directory and check for files under `/proc/systemtap` before deleting it. ([BZ#510282](#)<sup>2074</sup>)
- The `tcpmib.stp` and `ipmib.stp` tapsets have been updated to provide per-socket network statistics and dynamic TCP connection tracing. ([BZ#512202](#)<sup>2075</sup>)
- SystemTap now supports signal-based log file switching. As such, the on-file flight recorder can easily backup its latest logs on-the-fly. ([BZ#517091](#)<sup>2076</sup>)
- Using `SIGKILL` on the `stap` process will not terminate its child process, `stapio`. As such, users may not be aware that a SystemTap module is still probing the system, which will result in performance degradation. This update adds a note in `man stap` warning users of this behavior. ([BZ#523356](#)<sup>2077</sup>)
- Previous updates to SystemTap changed the order of parameters in the output of `stap`. This could cause problems in third-party tools that use SystemTap to probe kernel functions. This update reverts the order of parameters to its original sequence, which is also consistent with their order in the kernel source code. ([BZ#560890](#)<sup>2078</sup>)
- The `sys32_pipe` function was removed in updated kernels, but the system call tapsets for the `x86_64` kernel still contained an alias that used this function. As a result, using the probe `syscall.*` resulted in a semantic error. With this release, the system call tapsets for the `x86_64` kernel make the `syscall.pipe` probe alias (which uses `sys32_pipe`) optional, thereby avoiding the error. ([BZ#563114](#)<sup>2079</sup>)
- The `unprivileged user` mode in this release is stricter, carefully restricting the types of probes allowed for unprivileged users. In addition, `unprivileged user` mode also features clearer diagnostic messages whenever users attempt to use restricted probes. ([BZ#564443](#)<sup>2080</sup>)
- It was possible to call the module shutdown code while a start-up was in progress; this could leave some kernel callbacks registered after the module has unloaded. As such, running multiple



SystemTap scripts could crash the system. This update adds mutual exclusions to both shutdown and startup codes, thereby preventing a possible crash. ([BZ#521610](#)<sup>2081</sup>)

- The `literal_addr_to_sym_addr()` function did not correctly compute for marker addresses. As such, markers became inaccessible after running `prelink`; this prevented scripts that used markers from compiling. This release fixes the `literal_addr_to_sym_addr()`, ensuring that marker addresses are accessible after running `prelink`. ([BZ#564445](#)<sup>2082</sup>)
- Updates to GCC changed the format of variable locations it provided during compile time. However, the code used by SystemTap to process variable locations (in `loc2c.c`) was not updated accordingly to understand this new format. This could prevent some variables from initializing properly. With this release, the `loc2c.c` file is updated to correctly process the new format used by GCC for variable locations. ([BZ#536807](#)<sup>2083</sup>)

SystemTap users are advised to apply this update.

## 1.202. tar

### 1.202.1. RHSA-2010:0141: Moderate security update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2010:0141](#)<sup>2084</sup>

An updated tar package that fixes two security issues is now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The GNU tar program saves many files together in one archive and can restore individual files (or all of the files) from that archive.

A heap-based buffer overflow flaw was found in the way tar expanded archive files. If a user were tricked into expanding a specially-crafted archive, it could cause the tar executable to crash or execute arbitrary code with the privileges of the user running tar. ([CVE-2010-0624](#)<sup>2085</sup>)

Red Hat would like to thank Jakob Lell for responsibly reporting the [CVE-2010-0624](#)<sup>2086</sup> issue.

A denial of service flaw was found in the way tar expanded archive files. If a user expanded a specially-crafted archive, it could cause the tar executable to crash. ([CVE-2007-4476](#)<sup>2087</sup>)

Users of tar are advised to upgrade to this updated package, which contains backported patches to correct these issues.

### 1.202.2. RHBA-2010:0224: bug fix and enhancement update

An updated tar package that fixes several bugs and adds various enhancements is now available.

<sup>2085</sup> <https://www.redhat.com/security/data/cve/CVE-2010-0624.html>

<sup>2086</sup> <https://www.redhat.com/security/data/cve/CVE-2010-0624.html>

<sup>2087</sup> <https://www.redhat.com/security/data/cve/CVE-2007-4476.html>

The GNU tar program saves many files together in one archive and can restore individual files (or all of the files) from that archive.

This updated tar package provides fixes for the following bugs:

\* using the tar command's "-f [hostname]:[file]" option to specify a host on which to carry out operations on an archive failed with a "Cannot open: Input/output error" message. This error occurred when the rsh (remote shell) program was not available on the system on which the "tar" command was built. With this update, the tar package's spec file now lists the rsh package as a build dependency. Supplying the "-f [hostname]:[file]" option now works as expected. ([BZ#294661](https://bugzilla.redhat.com/show_bug.cgi?id=294661)<sup>2088</sup>)

\* the tar(1) man page incorrectly stated that the "--occurrence=N" option causes tar to process the first N occurrences of each file in the archive. The man page has been updated to reflect the actual behavior, which is to process only the Nth occurrence of each file in the archive. ([BZ#429522](https://bugzilla.redhat.com/show_bug.cgi?id=429522)<sup>2089</sup>)

\* extracting a tar archive that had been created using the "--xattrs" flag, which saves extended attribute information to the file, resulted in tar displaying "Warning: Cannot acl\_from\_text: Invalid argument" error messages for many extracted files. This was caused by an off-by-one coding error, and has been fixed in this update so that extended attributes are restored correctly from archive files. ([BZ#472553](https://bugzilla.redhat.com/show_bug.cgi?id=472553)<sup>2090</sup>)

\* the tar command's "--keep-newer-files" flag informs tar not to replace existing files that are newer than their archive copies. When restoring from an archive while using this option, tar incorrectly removed older files. With this update, tar does not remove older files when the "--keep-newer-files" flag is used to restore an archive. ([BZ#495686](https://bugzilla.redhat.com/show_bug.cgi?id=495686)<sup>2091</sup>)

\* extracting files from a tar archive when using the "--no-wildcards" flag to disable wildcard character interpretation did not work as expected: wildcard characters such as '\*', '[' and '?' still affected file name matches. With this update, the "--no-wildcards" flag correctly disables wildcard syntax so that file names are matched literally. ([BZ#510714](https://bugzilla.redhat.com/show_bug.cgi?id=510714)<sup>2092</sup>)

\* creating a tar archive which contained one or more directories with default extended attributes set, and then extracting that archive using the "--xattrs" flag on an Access Control List-enabled file system, did not result in the restoration of those directories' extended attributes. This has been fixed in this update so that directories' extended attributes are retained as expected when the tar archive is created and extracted appropriately. ([BZ#512097](https://bugzilla.redhat.com/show_bug.cgi?id=512097)<sup>2093</sup>)

\* installing the tar package with the "rpm -i --excludedocs" command resulted in "install-info: No such file or directory" error messages. With this update, installing tar while excluding files marked as documentation completes successfully, and without error messages. ([BZ#530955](https://bugzilla.redhat.com/show_bug.cgi?id=530955)<sup>2094</sup>)

\* attempting to extract a file smaller than 512 bytes from a tar archive resulted in an exit code of 0, indicating success, even though such files are not valid archives. With this update, tar returns an exit code of 2 and displays an error message when attempting to extract too-small files. ([BZ#544427](https://bugzilla.redhat.com/show_bug.cgi?id=544427)<sup>2095</sup>)

In addition, this updated package provides the following enhancements:

---

<sup>2088</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=294661](https://bugzilla.redhat.com/show_bug.cgi?id=294661)

<sup>2089</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=429522](https://bugzilla.redhat.com/show_bug.cgi?id=429522)

<sup>2090</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=472553](https://bugzilla.redhat.com/show_bug.cgi?id=472553)

<sup>2091</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=495686](https://bugzilla.redhat.com/show_bug.cgi?id=495686)

<sup>2092</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=510714](https://bugzilla.redhat.com/show_bug.cgi?id=510714)

<sup>2093</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=512097](https://bugzilla.redhat.com/show_bug.cgi?id=512097)

<sup>2094</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=530955](https://bugzilla.redhat.com/show_bug.cgi?id=530955)

<sup>2095</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=544427](https://bugzilla.redhat.com/show_bug.cgi?id=544427)

\* previously, tar's support for preserving metadata information on files and directories suffered from several limitations: the value of any extended attribute was limited to 5 bytes, and it was not possible to preserve SELinux context and extended attribute information on symbolic links. This update allows both kinds of information to be preserved for symlinks, and removes the 5-byte limit on extended attributes values. ([BZ#518208](#)<sup>2096</sup>)

\* the `gtar(1)` man page is newly included in this updated package. ([BZ#530956](#)<sup>2097</sup>)

Users are advised to upgrade to this updated tar package, which resolves these issues and adds these enhancements.

## 1.203. taskjuggler

### 1.203.1. RHBA-2009:1576: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2009:1576](#)<sup>2098</sup>

An updated taskjuggler package that fixes various bugs is now available.

TaskJuggler is a modern and powerful project management tool able to scale to projects with hundreds of resources and thousands of tasks. It covers the spectrum of project management tasks from first idea to completion of the project, and assists you during project scoping, resource assignment, cost and revenue planning, and risk and communication management.

This updated taskjuggler package includes fixes for the following bugs:

\* building TaskJuggler using the source RPM could fail on a multicore machine due to a timing problem with the building of the documentation. For this reason, multi-threaded builds have been disabled so that building TaskJuggler from the source RPM now succeeds. ([BZ#233028](#)<sup>2099</sup>)

\* using the source RPM to build TaskJuggler could fail due to a dependency on an exact version of the `docbook-dtds` package. This version requirement has been relaxed and corrected so that building TaskJuggler from the source RPM succeeds as expected. ([BZ#233033](#)<sup>2100</sup>)

TaskJuggler users who build the package from source are advised to upgrade to this updated package, which resolves these issues.

<sup>2096</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=518208](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=518208)

<sup>2097</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=530956](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=530956)

<sup>2099</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=233028](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=233028)

<sup>2100</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=233033](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=233033)

## 1.204. tcpdump

### 1.204.1. RHBA-2009:1605: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTRACK errata [RHBA-2009:1605](#)<sup>2101</sup>

Updated tcpdump packages that fix two bugs are now available.

The tcpdump tool is a command line utility for monitoring network traffic.

These updated packages resolve the following issues:

\* when run on 64-bit architectures, tcpslice read the timestamps in pcap files as 64-bit values despite them always been stored as 32-bit. Consequently, rather than extracting packet-trace file portions as expected, tcpslice returned a "couldn't find final packet in file" error. With this update tcpslice reads pcap timestamps as 32-bit values and now works as expected on 64-bit architectures. ([BZ#485670](#)<sup>2102</sup>)

\* running "tcpdump -i [n]", where [n] was an invalid interface index, caused tcpdump to SEGFAULT rather than return an "Invalid adapter index" error. tcpdump now explicitly checks for the last entry in the device list. If the [n] specified is higher than this entry, it returns "Invalid adapter index" as expected and does not crash. ([BZ#497819](#)<sup>2103</sup>)

All tcpdump users should upgrade to these updated packages, which resolve these issues.

## 1.205. tcsh

### 1.205.1. RHBA-2009:1494: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1494](#)<sup>2104</sup>

An updated tcsh package that fixes a bug is now available.

Tcsh is an enhanced and compatible version of the C shell (csh). Tcsh is a command language interpreter, which can be used as an interactive login shell, as well as a shell script command processor.

This updated tcsh package fixes the following bug:

\* when using the tcsh shell, running a command containing glob characters (such as "echo FAIL \*", for example) within a directory in which automount mounted other directories (such as for NIS) based

---

<sup>2102</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=485670](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=485670)

<sup>2103</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=497819](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=497819)

on a wildcard entry in the automount map file caused the service to attempt to mount those directories and fail, thereby increasing network traffic and system load. This update provides a fix to tcsh glob-handling so that using globbing characters as in the above example no longer triggers automount, thus resolving the issue. ([BZ#526459](#)<sup>2105</sup>)

All users of tcsh are advised to upgrade to this updated package, which resolves this issue.

## 1.205.2. RHBA-2010:0027: bug fix update



### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2010:0027](#)<sup>2106</sup>

An updated tcsh package that fixes a bug is now available.

Tcsh is an enhanced and compatible version of the C shell (csh). Tcsh is a command language interpreter, which can be used as an interactive login shell, as well as a shell script command processor.

This updated tcsh package fixes the following bug:

\* when using the tcsh shell, running a command with glob characters which also took as an argument any single- or double-quoted string resulted in a backslash character being inserted before every character in the quoted string arguments. This update provides a fix to tcsh glob-handling so that characters in single- or double-quoted string arguments are handled correctly and as expected. ([BZ#547529](#)<sup>2107</sup>)

All users of tcsh are advised to upgrade to this updated package, which resolves this issue.

## 1.205.3. RHBA-2010:0190: bug fix update

An updated tcsh package that fixes various bugs is now available.

Tcsh is an enhanced and compatible version of the C shell (csh). Tcsh is a command language interpreter, which can be used as an interactive login shell, as well as a shell script command processor.

This update package addresses the following bugs:

\* The local variable for "%j" within the prompt was incorrect, mistakenly referencing an unrelated global variable. This caused the entire prompt to be set to 0. Correcting the local variable ensures that when the "%j" character is included in a prompt it produces a 0 within the prompt, instead of setting the entire prompt to 0. ([BZ#461836](#)<sup>2108</sup>)

\* A previous patch for tcsh changed designed behavior in what was thought to be a bug fix. It was previously thought that the circumstance of a range being empty because the second argument was omitted or was in range, was an error. The behavior that was said to be a bug has since been found

<sup>2105</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=526459](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=526459)

<sup>2107</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=547529](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=547529)

<sup>2108</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=461836](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=461836)

to be documented as a feature. This updated package restores the behavior that allows a range to be empty if the second argument is omitted or is in range. (BZ#495642<sup>2109</sup>)

\* Invalid automount attempts occurred when using tcsh as a shell and globbing. This could have caused a slow down in computer operations. The bug is fixed in these updated packages by ensuring that when tcsh is being used with globbing, no incorrect automounts occur. (BZ#498625<sup>2110</sup>, BZ#526712<sup>2111</sup>)

\* Multi-byte characters were not always printed correctly by tcsh. The bug was located in the short2qstr() method that maintains a pointer to an internal buffer and it relocates the buffer if needed. Once the new buffer was allocated, the pointer would be incorrectly set to point to the beginning of a new memory block. Since the beginning of a new block may not be the end of a previous character, the last character could have been overwritten. This error is corrected by ensuring that the pointer moves to reference a memory space that is after the last character instead of just moving to the beginning of the next block. (BZ#502474<sup>2112</sup>)

\* Globbing was not processed correctly by tcsh when be used by the echo command. The consequence of this was that text echoed in quotation marks (" or ') would output with backslash characters in the text. This bug has been fixed by modifying the previous glob-automount patch to deal correctly with quoted text in an echo command. (BZ#529425<sup>2113</sup>)

\* Expansion of multiple filename globs failed if any glob in a command line expression failed. The correct behavior outlines that a glob command should only fail if all components of the command fail. This behavior is restored with this updated package. (BZ#529703<sup>2114</sup>)

All users of tcsh are advised to upgrade to this updated package, which resolves these issues.

## 1.206. tog-pegasus

### 1.206.1. RHEA-2010:0233: enhancement update

An enhanced tog-pegasus package is now available.

OpenPegasus Wbem Services for Linux enables management solutions that deliver increased control of enterprise resources. Wbem is a platform and resource independent DMTF standard that defines a common information model and communication protocol for monitoring and controlling resources from diverse sources.

This update includes the following enhancements:

\* The updated tog-pegasus package is rebased to upstream version 2.9.1. (BZ#518077<sup>2115</sup>)

The OpenPegasus Feature Status page summarizes the changes made in this version, <http://www.openpegasus.org/page.tpl?CALLER=index.tpl&ggid=799> .

\* when being installed, the tog-pegasus package displayed a warning message about the possibility of repository corruption occurring. This is because the post install stage ran the command cimmofl to

---

<sup>2109</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=495642](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=495642)

<sup>2110</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=498625](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=498625)

<sup>2111</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=526712](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=526712)

<sup>2112</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=502474](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=502474)

<sup>2113</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=529425](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=529425)

<sup>2114</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=529703](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=529703)

<sup>2115</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=518077](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=518077)

update the repository. This message is technically accurate but misleading as the chance of corruption is remote and there is no way to avoid it. The package SPEC file has been updated to include the `-W` parameter when running `cimmofl` in the post install stage. The warning message is no longer displayed. ([BZ#529161](#)<sup>2116</sup>)

Users of OpenPegasus should upgrade to this updated package, which adds these enhancements.

## 1.207. util-linux

### 1.207.1. RHBA-2010:0052: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2010:0052](#)<sup>2117</sup>

Updated util-linux packages that address a bug preventing fdisk from creating partitions starting beyond 1 TB are now available.

The util-linux package contains a large variety of low-level system utilities that are necessary for a Linux system to function. Among others, util-linux contains the fdisk partitioning tool.

The updated packages address the following problem:

\* a signed int in fdisk's `add_partition` function meant fdisk was unable to create a partition if the new partition's starting cylinder was beyond one terabyte. With this update, the pertinent value is now an unsigned long and fdisk can create partitions with starting cylinders beyond 1 terabyte, as expected. ([BZ#471372](#)<sup>2118</sup>)

util-linux users should upgrade to these updated packages, which resolve this issue.

## 1.208. valgrind

### 1.208.1. RHBA-2010:0272: bug fix and enhancement update

A Valgrind update that re-bases to upstream version 3.5.0, adds support for new Intel64/AMD64 instructions, and fixes several bugs is now available.

Valgrind is a tool to help you find memory-management problems in your programs. When a program is run under Valgrind's supervision, all reads and writes of memory are checked, and calls to `malloc/new/free/delete` are intercepted. As a result, Valgrind can detect a lot of problems that are otherwise very hard to find/diagnose.

This update re-bases Valgrind to upstream version 3.5.0 ([BZ#522330](#)<sup>2119</sup>), and applies several enhancements and fixes including the following:

<sup>2116</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=529161](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=529161)

<sup>2118</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=471372](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=471372)

<sup>2119</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=522330](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=522330)



\* Valgrind now supports `cmpxchg` instructions. This allows Valgrind to profile code that uses the Intel `cmpxchg` instruction. ([BZ#476271](#)<sup>2120</sup>)

\* The rebase also adds emulation for the 0x67 address-size-override prefix and support for multiple 0x66 operand size prefixes. This prevents unexpected "unhandled instruction bytes" errors when using Valgrind to profile programs that use these prefixes. ([BZ#515768](#)<sup>2121</sup> and [BZ#530165](#)<sup>2122</sup>)

All Valgrind users should apply this update.

## 1.209. vconfig

### 1.209.1. RHBA-2009:1573: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2009:1573](#)<sup>2123</sup>

An updated `vconfig` package that fixes two bugs is now available.

`Vconfig` is the utility for configuring 802.1q VLAN parameters.

This updated package fixes the following bugs:

\* although `vconfig` contains ELF objects, the `vconfig-debuginfo` package was empty. With this update the `-debuginfo` package contains valid debugging information as expected. ([BZ#500635](#)<sup>2124</sup>)

\* the previous `vconfig` release installed a CVS directory and related metadata to `/usr/share/doc/vconfig-1.9/contrib/`. They have been removed with this update. Note: this was a cosmetic issue only. The files did nothing and had no effect on `vconfig`'s utility. ([BZ#221161](#)<sup>2125</sup>)

Users of `vconfig` are advised to upgrade to this updated package, which resolves these issues.

## 1.210. vino

### 1.210.1. RHBA-2009:1590: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2009:1590](#)<sup>2126</sup>

---

<sup>2120</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=476271](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=476271)

<sup>2121</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=515768](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=515768)

<sup>2122</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=530165](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=530165)

<sup>2124</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=500635](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=500635)

<sup>2125</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=221161](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=221161)

An updated vino package that fixes a bug is now available.

Vino is a Virtual Network Computing (VNC) server for GNOME. It allows remote users to connect to a running GNOME session using VNC.

\* Vino incorrectly assumed the X shared memory extension would always provide support for shared memory pixmaps. This led to crashes with a BadImplementation error message. This update adds a check, ensuring shared memory pixmap support is available before requesting it. ([BZ#493097](https://bugzilla.redhat.com/show_bug.cgi?id=493097)<sup>2127</sup>)

All Vino users are advised to upgrade to these updated vino packages, which resolve this issue.

## 1.211. virt-manager

### 1.211.1. RHBA-2010:0281: bug fix update

An updated virt-manager package that fixes several bugs and adds an enhancement is now available.

Virtual Machine Manager (virt-manager) is a graphical tool for administering virtual machines for KVM, Xen, and QEMU. virt-manager can start, stop, add or remove virtualized devices, connect to a graphical or serial console, and see resource usage statistics for existing virtualized guests on local or remote machines. virt-manager uses the libvirt API.

This updated package addresses the following issues:

\* adding new isolated virtual networks could create broken or abnormal network configurations. The updated package provides better error handling for network creation. ([BZ#508273](https://bugzilla.redhat.com/show_bug.cgi?id=508273)<sup>2128</sup>)

\* various errors occurred after adding 19 volumes to the storage pool. ([BZ#508357](https://bugzilla.redhat.com/show_bug.cgi?id=508357)<sup>2129</sup>)

\* various virt-manager menus and menu items did not have keyboard shortcuts. ([BZ#509746](https://bugzilla.redhat.com/show_bug.cgi?id=509746)<sup>2130</sup>)

\* paused virtualized guests could be sent keys using the 'Send Key' options which could make paused virtualized guests shut down or restart. The 'Send Key' menu is now disabled if a virtualized guest is paused. ([BZ#509808](https://bugzilla.redhat.com/show_bug.cgi?id=509808)<sup>2131</sup>)

\* setting the "Autoconnect" option resulted in an error and virtualized guests consoles were not automatically opened. ([BZ#509985](https://bugzilla.redhat.com/show_bug.cgi?id=509985)<sup>2132</sup>)

\* migration from a remote host to a local host (both hosts connected to virt-manager) failed. The updated package resolves this issue and migrations to and from a local host work. ([BZ#510702](https://bugzilla.redhat.com/show_bug.cgi?id=510702)<sup>2133</sup>)

\* migrations were, in some cases, very slow with virt-manager for systems with multiple network interface cards of different speeds. The updated virt-manager has an advanced option which allows users to specify which IP address and port to use for a live migration. Specifying the fastest network interface will speed up migrations. ([BZ#518487](https://bugzilla.redhat.com/show_bug.cgi?id=518487)<sup>2134</sup>)

---

<sup>2127</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=493097](https://bugzilla.redhat.com/show_bug.cgi?id=493097)

<sup>2128</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=508273](https://bugzilla.redhat.com/show_bug.cgi?id=508273)

<sup>2129</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=508357](https://bugzilla.redhat.com/show_bug.cgi?id=508357)

<sup>2130</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=509746](https://bugzilla.redhat.com/show_bug.cgi?id=509746)

<sup>2131</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=509808](https://bugzilla.redhat.com/show_bug.cgi?id=509808)

<sup>2132</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=509985](https://bugzilla.redhat.com/show_bug.cgi?id=509985)

<sup>2133</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=510702](https://bugzilla.redhat.com/show_bug.cgi?id=510702)

<sup>2134</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=518487](https://bugzilla.redhat.com/show_bug.cgi?id=518487)

\* virt-manager did not save changes CPU or memory settings to the configuration files unless another feature was modified. In the updated package, changed memory and CPU settings are stored persistently. ([BZ#522096](#)<sup>2135</sup>)

\* specifying an address and port for a remote server using an unencrypted TCP connection caused VNC connections to fail. VNC connections work in the updated package when accessing remote hosts with the TCP connection type. ([BZ#534005](#)<sup>2136</sup>)

\* virt-manager did not persistently store new devices or changes to device configuration settings to the configuration files. virt-manager now makes devices persistent in configuration files when new devices are added. ([BZ#539496](#)<sup>2137</sup>)

\* a traceback error occurred in virt-manager caused by the retry\_login function. The updated package handles this error. ([BZ#436320](#)<sup>2138</sup>)

The updated package adds the following enhancements:

\* support for creating routed virtual networks with virt-manager. ([BZ#452644](#)<sup>2139</sup>)

All Virtual Machine Manager users should install this updated package which fixes bugs and adds an enhancement.

## 1.212. vixie-cron

### 1.212.1. RHBA-2009:1684: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1684](#)<sup>2140</sup>

An updated vixie-cron package that fixes a bug that prevented pam variables being set with cron jobs is now available.

The vixie-cron package contains the Vixie version of cron. Cron is a standard UNIX daemon that runs specified programs at scheduled times. The vixie-cron package adds improved security and more powerful configuration options to the standard version of cron.

This update fixes the following bug:

\* according to the pam man page, the cron daemon, crond, "supports access control with PAM" but the PAM configuration file for crond did not export environment variables correctly and, consequently, setting pam variables via cron did not work. This update includes a corrected `/etc/pam.d/crond` file that export environment variables correctly. Setting pam variables via cron now works as documented. ([BZ#546568](#)<sup>2141</sup>)

All vixie-cron users should upgrade to this updated package, which resolves this issue.

---

<sup>2135</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=522096](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=522096)

<sup>2136</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=534005](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=534005)

<sup>2137</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=539496](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=539496)

<sup>2138</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=436320](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=436320)

<sup>2139</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=452644](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=452644)

<sup>2141</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=546568](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=546568)

## 1.213. vsftpd

### 1.213.1. RHBA-2009:1664: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata *RHBA-2009:1664*<sup>2142</sup>

An updated vsftpd package that fixes a bug is now available.

The vsftpd package includes a Very Secure FTP (File Transfer Protocol) daemon.

This updated vsftpd package fixes the following bug:

\* certain vsftpd commands such as "ls" accept wildcard (globbing) characters, which allows matching multiple files with a single command. However, these commands did not "expand" any wildcard characters beyond the first one in any given string, which could have caused a failure to match certain files. With this update, vsftpd's commands which accept wildcards now expand all such characters fully, thus enabling them to match file names as expected. (*BZ#544278*<sup>2143</sup>)

All users of vsftpd are advised to upgrade to this updated package, which resolves this issue.

## 1.214. wdaemon

### 1.214.1. RHEA-2010:0326: enhancement update

An enhanced wdaemon package that adds an enhancement is now available.

wdaemon is a helper application which emulates persistent input devices for Wacom tablets allowing them to be plugged-in and unplugged while an X.org server is running.

This updated wdaemon package upgrades wdaemon to version 0.14 which includes the following enhancement:

\* added support for Intuos4 Wacom tablets

All users of wdaemon are advised to upgrade to this updated package if they need this enhancement.

## 1.215. wget

### 1.215.1. RHSA-2009:1549: Moderate security update



#### Important

This update has already been released (prior to the GA of this release) as the security errata *RHSA-2009:1549*<sup>2144</sup>

<sup>2143</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=544278](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=544278)

An updated wget package that fixes a security issue is now available for Red Hat Enterprise Linux 3, 4, and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

GNU Wget is a file retrieval utility that can use HTTP, HTTPS, and FTP.

Daniel Stenberg reported that Wget is affected by the previously published "null prefix attack", caused by incorrect handling of NULL characters in X.509 certificates. If an attacker is able to get a carefully-crafted certificate signed by a trusted Certificate Authority, the attacker could use the certificate during a man-in-the-middle attack and potentially confuse Wget into accepting it by mistake. ([CVE-2009-3490](https://www.redhat.com/security/data/cve/CVE-2009-3490.html)<sup>2145</sup>)

Wget users should upgrade to this updated package, which contains a backported patch to correct this issue.

### 1.216. wpa\_supplicant

#### 1.216.1. RHBA-2010:0235: bug fix and enhancement update

Updated wpa\_supplicant packages that fix several bugs and add various enhancements are now available.

wpa\_supplicant is a WPA Supplicant for Linux, BSD and Windows with support for WPA and WPA2 (IEEE 802.11i / RSN). Supplicant is the IEEE 802.1X/WPA component that is used in the client stations. It implements key negotiation with a WPA Authenticator and it controls the roaming and IEEE 802.11 authentication/association of the wlan driver.

\* the wpa-supplicant package would enter a loop when used with Intel Wifi Link 3945, 4965, 5000-series and 6000-series devices. This resulted in those devices not being able to reconnect to the wireless access point successfully. A number of changes were made to the wpa\_supplicant package to ensure that the disconnection happens cleanly, and the effected devices can now reconnect successfully. ([BZ#506230](https://bugzilla.redhat.com/show_bug.cgi?id=506230)<sup>2146</sup>)

Users are advised to upgrade to this updated wpa\_supplicant package, which resolves this issue.

### 1.217. xen

#### 1.217.1. RHBA-2009:1514: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1514](https://errata.redhat.com/errata/RHBA-2009:1514)<sup>2147</sup>

Updated xen packages that close a memory leak in xend are now available.

---

<sup>2145</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3490.html>

<sup>2146</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=506230](https://bugzilla.redhat.com/show_bug.cgi?id=506230)

Xen is a high performance and secure open source virtualization framework. Virtualization allows users to run guest operating systems in virtual machines on top of a host operating system.

These updated xen packages fix the following bug:

\* issuing an "xm info" command or any virsh commands caused xend to leak memory. As well, xend's memory consumption grew very quickly in combination with cluster suite, which uses virsh to monitor running guests. This update fixes the underlying errors in the PyList\_Append and PyDict\_SetItemString functions that caused the memory leaks. ([BZ#528163](#)<sup>2148</sup>)

All xen users are advised to upgrade to these updated packages, which resolve this issue. Note: after installation, the xend service must be restarted for this update to take effect.

### 1.217.2. RHBA-2010:0010: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2010:0010](#)<sup>2149</sup>

Updated xen packages that close a memory leak in xend are now available.

Xen is a high-performance and secure open source virtualization framework. Virtualization allows users to run guest operating systems in virtual machines on top of a host operating system.

These updated xen packages fix the following bug:

\* following a guest shutdown, attempting to recreate that guest may have failed due to timing issues, which caused the xend daemon to think that the guest name was still in use, even though it was not. Also, the "xm list" command (correctly) did not show the name of the guest which had shut down. As a temporary workaround, running the "xm list" command once would rectify this situation so that the guest with the same name as the one which had been shut down could be recreated. This update resolves this issue so that a guest with the same name as a guest which has recently been shut down can be recreated immediately, without having to run an interim command. ([BZ#547289](#)<sup>2150</sup>)

Xen users are advised to upgrade to these updated packages, which resolve this issue. Note: after installation, the xend service must be restarted for this update to take effect.

### 1.217.3. RHSA-2009:1472: Moderate security and bug fix update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2009:1472](#)<sup>2151</sup>

Updated xen packages that fix a security issue and multiple bugs are now available for Red Hat Enterprise Linux 5.

<sup>2148</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=528163](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=528163)

<sup>2150</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=547289](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=547289)

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

Xen is an open source virtualization framework. Virtualization allows users to run guest operating systems in virtual machines on top of a host operating system.

The pyGrub boot loader did not honor the "password" option in the grub.conf file for para-virtualized guests. Users with access to a guest's console could use this flaw to bypass intended access restrictions and boot the guest with arbitrary kernel boot options, allowing them to get root privileges in the guest's operating system. With this update, pyGrub correctly honors the "password" option in grub.conf for para-virtualized guests. ([CVE-2009-3525](https://www.redhat.com/security/data/cve/CVE-2009-3525.html)<sup>2152</sup>)

This update also fixes the following bugs:

\* rebooting para-virtualized guests sometimes caused those guests to crash due to a race condition in the xend node control daemon. This update fixes this race condition so that rebooting guests no longer potentially causes them to crash and fail to reboot. ([BZ#525141](https://bugzilla.redhat.com/show_bug.cgi?id=525141)<sup>2153</sup>)

\* due to a race condition in the xend daemon, a guest could disappear from the list of running guests following a reboot, even though the guest rebooted successfully and was running. This update fixes this race condition so that guests always reappear in the guest list following a reboot. ([BZ#525143](https://bugzilla.redhat.com/show_bug.cgi?id=525143)<sup>2154</sup>)

\* attempting to use PCI pass-through to para-virtualized guests on certain kernels failed with a "Function not implemented" error message. As a result, users requiring PCI pass-through on para-virtualized guests were not able to update the xen packages without also updating the kernel and thus requiring a reboot. These updated packages enable PCI pass-through for para-virtualized guests so that users do not need to upgrade the kernel in order to take advantage of PCI pass-through functionality. ([BZ#525149](https://bugzilla.redhat.com/show_bug.cgi?id=525149)<sup>2155</sup>)

All Xen users should upgrade to these updated packages, which contain backported patches to correct these issues. After installing the updated packages, the xend service must be restarted for this update to take effect.

### 1.217.4. RHBA-2010:0294: bug fix and enhancement update

The **xen** packages contain tools for managing the virtual machine monitor in Red Hat Enterprise Linux Virtualization.

These updated packages fix the following bugs:

- Cause: Fully-virtualized Fedora 10 and newer guests would freeze during the boot sequence. The guest would repeatedly receive an error similar to the following error:

```
ata2.00: configured for MWDMA2
ata2: EH complete
ata2.00: exception Emask 0x0 SAct 0x0 SErr 0x0 action 0x6 frozen
ata2.00: cmd a0/00:00:00:00:00:00/00:00:00:00/a0 tag 0
        cdb 1e 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        res 41/20:03:00:00:00:00/00:00:00:00/a0 Emask 0x3 (HSM violation)
ata2.00: status: { DRDY ERR -}
ata2: soft resetting link
```

---

<sup>2152</sup> <https://www.redhat.com/security/data/cve/CVE-2009-3525.html>

<sup>2153</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=525141](https://bugzilla.redhat.com/show_bug.cgi?id=525141)

<sup>2154</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=525143](https://bugzilla.redhat.com/show_bug.cgi?id=525143)

<sup>2155</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=525149](https://bugzilla.redhat.com/show_bug.cgi?id=525149)



The updated packages resolve this issue by fixing the virtualized ATA driver. The updated packages cause the following issue on the guest:

```
ata2.00: exception Emask 0x0 SAct 0x0 SErr 0x0 action 0x6 frozen
ata2.00: BMDMA stat 0x5
ata2.00: cmd a0/01:00:00:80:00/00:00:00:00/a0 tag 0 dma 16512 in
ata2.00: status: { DRDY DRQ -}
ata2: soft resetting link
ata2.00: configured for MWDMA2
ata2: EH complete
```

After this error the guest should successfully boot. ([BZ#480317](#)<sup>2156</sup>)

- The Xen daemon would hang if a user attempted to shut down or save a paused guest. Guests cannot be saved or shut down if the guest is in a paused state as those operations can only be conducted on running guests. The updated Xen daemon will no longer hang but the user is presented with the following warning:

```
Error: Can't shutdown/save the domain since the domain is paused; unpaused it first if you
want to shutdown/save
```

To shut down or save a guest in a paused state, the guest must first be unpaused by the user. ([BZ#504910](#)<sup>2157</sup>)

- Sufficient memory was not reserved for fully virtualized guests when creating new guests. Memory listed as available by the `xm info` command could not be fully allocated to the guest. When attempting create a fully virtualized guest with more than or equal to the maximum available memory value, the following error message would appear:

```
Error: (1, -'Internal error', -'Could not allocate memory for HVM guest.\n (16 = Device or
resource busy)')
```

This issue has been resolved by improving the memory balloon driver to correctly allocate memory for fully virtualized guests and fully virtualized guests using the Intel VT-d extensions for PCI passthrough. ([BZ#512041](#)<sup>2158</sup>)

- An error message appeared when attempting to detach a PCI device from a para-virtualized guest. The error is corrected in the updated packages. PCI passthrough is only supported by Xen full virtualization and not by para-virtualization. ([BZ#512307](#)<sup>2159</sup>)
- Scheduling was reset if a guest was saved and restored. Scheduling data is now preserved when a guest is saved and restored. ([BZ#513211](#)<sup>2160</sup>)
- A race condition between the `xend` daemon and the hotplug scripts caused a recently rebooted guest to disappear from the `xm list` command output. The race condition is fixed and guests will now always appear in the `xm list` command output after the guest is rebooted. ([BZ#513604](#)<sup>2161</sup>)
- The `xm pci-list` command would fail due to an unhandled error in the output parsing functions for para-virtualized guests. The output is now handled correctly by the `xm pci-list` command which resolves this issue in the updated packages. ([BZ#514025](#)<sup>2162</sup>)
- An uninformative error message appeared when the `xm pci-list-assignable-devices` command was executed. The `pciback` kernel module must be loaded before executing the `xm`

**pci-list-assignable-devices** command. The updated package provides an error that informs the user the module is not loaded. ([BZ#514448](#)<sup>2163</sup>)

- A race condition rarely occurred when a para-virtualized guest was rebooted. When the race condition occurred it caused para-virtualized guests to stop or crash after rebooting. The race condition no longer occurs in the updated packages and para-virtualized guests should always run after rebooting. ([BZ#518104](#)<sup>2164</sup>)
- The python environment has been changed to explicitly use the system python. This allows users to install other versions of python for testing. ([BZ#521333](#)<sup>2165</sup>)
- Fixed a regression which prevented para-virtualized guests from being started with attached PCI devices. PCI passthrough now works with para-virtualized guests. ([BZ#521346](#)<sup>2166</sup>)
- Using the value *rename-restart* for the *on\_reboot* parameter caused guests to not start when the guest was rebooted. Using *rename-restart* now causes guests to start successfully after a reboot with a different name. ([BZ#521799](#)<sup>2167</sup>)
- Simultaneous migrations from two hosts to a third host and two hosts simultaneously swapping guests between them would fail. The updated packages fix this issue and simultaneous migrations now work between multiple hosts. ([BZ#522850](#)<sup>2168</sup>)
- Memory leaks in the **libxc** and the **libxenstore** python binding libraries caused increasing memory usage over time. The memory leaks in the **libxc** and the **libxenstore** libraries are fixed in the updated package and the libraries memory usage should remain steady. ([BZ#524308](#)<sup>2169</sup>)
- A guest name conflict caused a running guest to appear shut down after restarting the guest. This issue is resolved in the updated package and running guest do not erroneously report that they are shut down. ([BZ#529880](#)<sup>2170</sup>)
- The **xm dump-core** command could not dump memory while a guest is running. The memory dump functionality has been improved, however, there are still issues with generating live dumps. The guest core dump image may be in an inconsistent state if the guest is under load. Users are now warned about this issue. ([BZ#382591](#)<sup>2171</sup>)

These updated packages add the following enhancements:

- PCI device hotplugging works in the updated packages. This feature is supported by the **libvirt** and **virt-manager** tools. ([BZ#512315](#)<sup>2172</sup>)
- Support for MSI-X mask bit acceleration. MSI-X mask bit acceleration improves performance of SR-IOV devices. ([BZ#557446](#)<sup>2173</sup> and [BZ#542756](#)<sup>2174</sup>)
- The **xendomains** service now has less confusing and better formatted output. ([BZ#251666](#)<sup>2175</sup>)
- Support for the *maxvcpus* parameter for Xen configuration files. The *maxvcpus* parameter sets a maximum number of VCPUs available that is separate from the initial VCPUs assigned to the guest. ([BZ#453042](#)<sup>2176</sup>)
- The SMBIOS device, the BIOS device for virtualized guests, now presents the device manufacturer as "Red Hat" and the product family as "Red Hat Enterprise Linux". ([BZ#499453](#)<sup>2177</sup>)
- SCSI emulated devices were not supported in prior versions. Emulated SCSI devices are now supported. ([BZ#515757](#)<sup>2178</sup>)

- Support for assigning more than 12 SR-IOV Virtual Functions (VFs) to a single fully virtualized Xen guest. ([BZ#511403](#)<sup>2179</sup>)
- Support for BZIP2 and LZMA compressed kernels for para-virtualized guests. ([BZ#517049](#)<sup>2180</sup>)
- PCIe switches allow peer to peer transactions that are routed by the switch and could bypass the Intel VT-d translation hardware, potentially causing unexpected behavior in the system. Access Control Services (ACS) allows the system to force the PCIe switch to route all traffic upstream so that the VT-d hardware can validate all transactions. The updated package prevents assigning PCI devices below a non-ACS PCIe switch. ([BZ#523819](#)<sup>2181</sup>)
- Support for using the EXT4 file system for a boot partition for para-virtualized guests. ([BZ#524611](#)<sup>2182</sup>)
- SMBIOS now complies with the Microsoft Server Virtualization Validation Program (SVVP). ([BZ#540161](#)<sup>2183</sup>)
- Xen now automatically pins guests to a smallest possible number of NUMA nodes. This provides better performance on NUMA based systems. ([BZ#543199](#)<sup>2184</sup>)

Users of xen are advised to upgrade to these updated packages, which resolve these issues and add these enhancements.

## 1.218. xerces-j2

### 1.218.1. RHSA-2009:1615: Moderate security update



#### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2009:1615](#)<sup>2185</sup>

Updated xerces-j2 packages that fix a security issue are now available for Red Hat Enterprise Linux 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The xerces-j2 packages provide the Apache Xerces2 Java Parser, a high-performance XML parser. A Document Type Definition (DTD) defines the legal syntax (and also which elements can be used) for certain types of files, such as XML files.

A flaw was found in the way the Apache Xerces2 Java Parser processed the SYSTEM identifier in DTDs. A remote attacker could provide a specially-crafted XML file, which once parsed by an application using the Apache Xerces2 Java Parser, would lead to a denial of service (application hang due to excessive CPU use). ([CVE-2009-2625](#)<sup>2186</sup>)

Users should upgrade to these updated packages, which contain a backported patch to correct this issue. Applications using the Apache Xerces2 Java Parser must be restarted for this update to take effect.

<sup>2186</sup> <https://www.redhat.com/security/data/cve/CVE-2009-2625.html>

### 1.219. xmlsec1

#### 1.219.1. RHSA-2009:1428: Moderate security update



##### Important

This update has already been released (prior to the GA of this release) as the security errata [RHSA-2009:1428](#)<sup>2187</sup>

Updated xmlsec1 packages that fix one security issue are now available for Red Hat Enterprise Linux 4 and 5.

This update has been rated as having moderate security impact by the Red Hat Security Response Team.

The XML Security Library is a C library based on libxml2 and OpenSSL. It implements the XML Signature Syntax and Processing and XML Encryption Syntax and Processing standards. HMAC is used for message authentication using cryptographic hash functions. The HMAC algorithm allows the hash output to be truncated (as documented in RFC 2104).

A missing check for the recommended minimum length of the truncated form of HMAC-based XML signatures was found in xmlsec1. An attacker could use this flaw to create a specially-crafted XML file that forges an XML signature, allowing the attacker to bypass authentication that is based on the XML Signature specification. ([CVE-2009-0217](#)<sup>2188</sup>)

Users of xmlsec1 should upgrade to these updated packages, which contain a backported patch to correct this issue. After installing the updated packages, applications that use the XML Security Library must be restarted for the update to take effect.

### 1.220. xorg-x11-drivers

#### 1.220.1. RHEA-2010:0323: enhancement update

An updated xorg-x11-drivers package that adds an enhancement is now available.

xorg-x11-drivers is a metapackage that pulls in all the X drivers typically required for a particular platform.

This updated package adds the following enhancement:

\* The qxl driver is added to i386, AMD64 and Intel 64 platforms. qxl is an accelerated paravirtualized graphics device in Red Hat's KVM virtualization platform.

All users should upgrade to this updated package, which adds this enhancement.

---

<sup>2188</sup> <https://www.redhat.com/security/data/cve/CVE-2009-0217.html>

## 1.221. xorg-x11-drv-ast

### 1.221.1. RHEA-2010:0202: enhancement update

An enhanced xorg-x11-drv-ast package is now available.

The xorg-x11-drv-ast package is the Xorg X11 ast video driver. It is used to drive ASpeedTech graphics cards for the Xorg implementation of the X Window System.

\* the xorg-x11-drv-ast package has been updated to provide support for the ASpeedTech 1100, 2050, 2100, 2150, and 2200 graphics parts. ([BZ#488274](#)<sup>2189</sup>)

All ASpeedTech graphics card users should upgrade to this updated package, which adds support for this hardware.

## 1.222. xorg-x11-drv-evdev

### 1.222.1. RHBA-2010:0246: bug fix update

Updated xorg-x11-drv-evdev packages that fix a potential division by zero bug are now available.

The xorg-x11-drv-evdev packages provide an X input device driver that lets the X server read input events from the evdev kernel interface.

This update applies the following bug fixes:

\* an invalid axis range can result in a division by zero error upon moving the mouse, crashing the X server. ([BZ#371151](#)<sup>2190</sup>)

\* the release string in the spec file for the packages has changed from %{dist} to %{?dist}. ([BZ#548008](#)<sup>2191</sup>)

All users of this package are advised to upgrade to these updated packages, which resolve these issues.

## 1.223. xorg-x11-drv-fbdev

### 1.223.1. RHBA-2010:0203: bug fix and enhancement update

An updated xorg-x11-drv-fbdev package that fixes a bug is now available.

The xorg-x11-drv-fbdev package provides a driver for Linux kernel framebuffer devices for use with the X.Org implementation of the X Window System. This driver is normally only used when a native X.Org driver is not available.

\* the framebuffer driver had a bug relating to CopyArea performance, which led to the system appearing to run extremely slowly. The performance bug was corrected in an upstream version of the driver and the sluggish performance is no longer seen. ([BZ#466163](#)<sup>2192</sup>)

---

<sup>2189</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=488274](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=488274)

<sup>2190</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=371151](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=371151)

<sup>2191</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=548008](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=548008)

<sup>2192</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=466163](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=466163)

Users are advised to upgrade to this updated xorg-x11-drv-fbdev package, which resolves this issue.

### 1.224. xorg-x11-drv-i810

#### 1.224.1. RHBA-2010:0262: bug fix and enhancement update

Updated xorg-x11-drv-i810 packages that fix several bugs and add various enhancements are now available.

xorg-x11-drv-i810 is an Intel integrated graphics video driver for the X.Org implementation of the X Window System.

Note that this package provides two drivers, 'i810' and 'intel'. The i810 driver is supported for i8xx series chips, up to and including i865. The intel driver is supported for all i915 and later chips.

These updated packages resolve the following bugs:

\* previously, there was an issue in the CRT detect code in the driver. Consequently, after updating the xorg-x11-drv-i810 package, the X server may have failed to boot, returning the error message:

Caught signal 11. Server aborting

With this update, this issue has been resolved. ([BZ#521350](https://bugzilla.redhat.com/show_bug.cgi?id=521350)<sup>2193</sup>)

\* previously, using xrandr to change the screen resolution of a video device under the Intel Q43/Q45 chipset sometimes failed. After attempting the switch, the screen may have blanked and gone out of sync. With this update, this issue has been resolved. ([BZ#511896](https://bugzilla.redhat.com/show_bug.cgi?id=511896)<sup>2194</sup>)

Additionally, these updated packages provide the following enhancements:

\* 2D support for the integrated graphics device found in Intel Core i3, Core i5 and Core i7 processors. ([BZ#517356](https://bugzilla.redhat.com/show_bug.cgi?id=517356)<sup>2195</sup>) \* support for the integrated graphics in the Intel B43 chipset. ([BZ#525276](https://bugzilla.redhat.com/show_bug.cgi?id=525276)<sup>2196</sup>)

All xorg-x11-drv-i810 users should upgrade to these updated package which provides these bug fixes and enhancements.

### 1.225. xorg-x11-drv-mga

#### 1.225.1. RHBA-2010:0324: bug fix update

An updated xorg-x11-drv-mga driver which fixes several bugs is now available.

xorg-x11-drv-mga is a video driver for the X.Org implementation of the X Window System, for Matrox G-series chips.

This updated package addresses the following issues:

\* Updates to the driver for Pilot1 and Pilot2 chipsets caused display errors in the installer for the remote kernel-based virtual machine when used with the Pilot2 chipset at 800x600 resolution. This

---

<sup>2193</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=521350](https://bugzilla.redhat.com/show_bug.cgi?id=521350)

<sup>2194</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=511896](https://bugzilla.redhat.com/show_bug.cgi?id=511896)

<sup>2195</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=517356](https://bugzilla.redhat.com/show_bug.cgi?id=517356)

<sup>2196</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=525276](https://bugzilla.redhat.com/show_bug.cgi?id=525276)

patch adds a condition that the updates are used only with the Pilot1 chipset, and no longer causes display issues. ([BZ#518997](#)<sup>2197</sup>)

\* When kernel panic was initiated on a machine with a Matrox video controller, the system would freeze and fail to generate a vmcore. This was caused by a bug in DDC1 (Display Data Channel) support or the Matrox G200eW video card. The DDC1 support that caused the problem has been removed. The vmcore file now generates correctly. ([BZ#563196](#)<sup>2198</sup>)

Users are advised to upgrade to this updated xorg-x11-drv-mga package which resolves these issues.

## 1.226. xorg-x11-drv-nv

### 1.226.1. RHBA-2010:0204: bug fix and enhancement update

An updated xorg-x11-drv-nv package that fixes a bug and adds support for Quadro FX 770M, FX1800M and 880M GPUs is now available.

xorg-x11-drv-nv provides a driver for NVIDIA cards for the X.org implementation of the X Window System.

This update resolves the following issue:

\* previously, xorg-x11-drv-nv specified no explicit range for offscreen Pixmaps. On rare occasions, this caused X to crash with a sig 11 error when Firefox 3.5.x attempted to load certain, specific, web pages (eg <http://adorama.com>). With this update, explicit 512 pixel limits have been placed on offscreen Pixmap width and height. Consequently, xorg-x11-drv-nv no longer causes X to crash when Firefox 3.5 loads the specified pages. ([BZ#498500](#)<sup>2199</sup>)

This update also adds the following enhancements:

\* previously, the NVIDIA cards that used the Quadro FX 770M GPU were driven as generic VESA-compliant video cards. With this update, the xorg-x11-drv-nv driver adds Quadro FX 770M support. Amongst other improvements, Quadro FX 770M-based cards now support multi-head setups. ([BZ#486135](#)<sup>2200</sup>, [BZ#499684](#)<sup>2201</sup>)

\* this update adds support for the NVIDIA Quadro FX 1800M or 880M GPUs such as are included in Dell M4500 Mobile Workstations. ([BZ#514999](#)<sup>2202</sup>)

All users should install this newly released package, which resolves these issues.

## 1.227. xorg-x11-drv-qxl

### 1.227.1. RHBA-2010:0188: bug fix update

An updated xorg-x11-drv-qxl package that fixes numerous bugs is now available.

<sup>2197</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=518997](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=518997)

<sup>2198</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=563196](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=563196)

<sup>2199</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=498500](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=498500)

<sup>2200</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=486135](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=486135)

<sup>2201</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=499684](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=499684)

<sup>2202</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=514999](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=514999)



xorg-x11-qxl-drv is an X11 video driver for the QEMU QXL video accelerator. This driver makes it possible to use Red Hat Enterprise Linux 5 as a guest operating system under KVM and QEMU, using the SPICE protocol.

This update addresses the following:

- \* if a virtual machine running X11 was switched to run-level 3 and the startx command was then used to restart X11, the X server would hang, resulting in a black screen. When "init 3" is run, the QXL device switches into VGA mode without either notifying the X server or clearing the command buffer. As a consequence, when X attempted to restart, the commands queued from the previous X session (which are cleared when an X session is stopped properly and safely) cause X to hang and the virtual machine to crash.

With this update the QXL driver now checks the device mode before issuing any commands: if the QXL driver reports being in VGA mode, the driver now waits for it to be set back to non-VGA mode as part of the normal X startup process. This avoids the problem created by the QXL device and ensures the command queue is not left in an illegal state when exiting X. ([BZ#509410](https://bugzilla.redhat.com/show_bug.cgi?id=509410)<sup>2203</sup>)

- \* In the previous release, only a 32-bit x86 version of the QXL driver was included. With this update both 32-bit and 64-bit x86 versions are provided. ([BZ#543663](https://bugzilla.redhat.com/show_bug.cgi?id=543663)<sup>2204</sup>)

- \* Launching applications from shortcuts pinned to the task bar panel caused a visual glitch where rectangles animating the movement of windows would persist on screen.

To improve performance and fix bugs in conjunction with moving windows around, the driver was modified to keep damage in a separate pending\_copy region. Accelerated operations then delete this region, and whenever new damage appears, it is unioned onto the "to\_be\_sent" region, which is then submitted at BlockHandler time. ([BZ#544781](https://bugzilla.redhat.com/show_bug.cgi?id=544781)<sup>2205</sup>)

This modification also resolves the following:

- \* Scrolling through a document with the mouse wheel in OpenOffice 3.1.1 would cause corruption of the displayed document text. ([BZ#552181](https://bugzilla.redhat.com/show_bug.cgi?id=552181)<sup>2206</sup>)

- \* In Red Hat Enterprise Linux 5.4 with the KDE desktop running in a virtual machine using the QXL driver, dragging icons or drawing frames on the desktop with the mouse would result in residual screen corruption. ([BZ#552838](https://bugzilla.redhat.com/show_bug.cgi?id=552838)<sup>2207</sup>)

- \* When running x11perf in a virtual machine with the 32-bit QXL driver, X Windows would occasionally become unresponsive though the VM was responsive otherwise.

The 32-bit QXL driver did not implement correct memory accesses to the QXL ring buffer. This could lead to an endless loop. In this update, all ring accesses have been modified to use volatile accessors. The driver no longer enters an endless loop after this modification. ([BZ#549379](https://bugzilla.redhat.com/show_bug.cgi?id=549379)<sup>2208</sup>)

- \* Unmapping errors and incorrect draw area values appeared in the log file.

This was caused by incorrect size parameters applied to xf86UnMapVidMem and printing of values from incorrect memory structure. The size parameter was modified and ROM structure replaced QXL structure for draw area values. These errors no longer appear in the log. ([BZ#549386](https://bugzilla.redhat.com/show_bug.cgi?id=549386)<sup>2209</sup>)

---

<sup>2203</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=509410](https://bugzilla.redhat.com/show_bug.cgi?id=509410)

<sup>2204</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=543663](https://bugzilla.redhat.com/show_bug.cgi?id=543663)

<sup>2205</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=544781](https://bugzilla.redhat.com/show_bug.cgi?id=544781)

<sup>2206</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=552181](https://bugzilla.redhat.com/show_bug.cgi?id=552181)

<sup>2207</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=552838](https://bugzilla.redhat.com/show_bug.cgi?id=552838)

<sup>2208</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=549379](https://bugzilla.redhat.com/show_bug.cgi?id=549379)

<sup>2209</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=549386](https://bugzilla.redhat.com/show_bug.cgi?id=549386)

\* Video was not displayed to screen in video players.

The QXL driver did not output video streams with the correct effect type and consequently video was not displayed to screen. The driver was modified to use `QXL_EFFECT_OPAQUE` instead of `QXL_EFFECT_BLEND`. Video detection works correctly after this modification. ([BZ#551289](#)<sup>2210</sup>)

\* X11 crashed when the display configuration was changed to "thousands of colors" (16-bit color depth) and the virtual machine was restarted.

QXL uses a 15-bit color depth (x1r5g5b5) rather than 16-bits. The driver implemented 16-bit depth modes incorrectly with the "thousands of colors" setting and caused X11 to crash.

The driver was modified to implement a 15-bit color depth which allowed X11 to restart without crashing after "thousands of colors" was set in the display configuration. ([BZ#551981](#)<sup>2211</sup>)

All users of KVM-based virtualization are advised to upgrade to this updated package, which fixes these issues.

## 1.228. xorg-x11-drv-vesa

### 1.228.1. RHBA-2010:0312: bug fix update

An updated `xorg-x11-drv-vesa` driver which fixes a bug is now available.

`xorg-x11-drv-vesa` is a video driver for the X.Org implementation of the X Window System. It is used as a fallback driver for cards with no native driver, or when the native driver does not work.

On Dell Precision M09-family laptops using nVidia Quadro FX 770M video drivers, DPMS backlight power saving modes did not function correctly. The backlight would remain on when the laptop screen was closed, significantly reducing the standby life of the device. The update implements a change to the driver's DPMS settings, which corrects the backlight issue. ([BZ#494671](#)<sup>2212</sup>)

Users of the `xorg-x11-drv-vesa` package are advised to upgrade to the updated package, which resolves this issue.

## 1.229. xorg-x11-server

### 1.229.1. RHBA-2009:1691: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1691](#)<sup>2213</sup>

Updated `xorg-x11-server` packages that resolve an issue are now available.

X.org X11 is an open source implementation of the X Window System. It provides the basic low level functionality upon which full fledged graphical user interfaces such as GNOME and KDE are designed.

<sup>2210</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=551289](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=551289)

<sup>2211</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=551981](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=551981)

<sup>2212</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=494671](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=494671)

These updated xorg-x11-server packages fix the following bug:

\* when using a dual-head X11 configuration with more than one display, if the user's session was locked by gnome-screensaver, then clicking or typing only resulted in a black screen and a mouse pointer instead of a login prompt as expected. Because of this, it was not possible to log back in to the desktop session once gnome-screensaver had been started. This update restores the ability to log back into a session after gnome-screensaver has started when using a dual-head X11 configuration. ([BZ#537759](https://bugzilla.redhat.com/show_bug.cgi?id=537759)<sup>2214</sup>)

All users of xorg-x11-server are advised to upgrade to these updated packages, which resolve this issue.

### 1.229.2. RHBA-2010:0259: bug fix update

Updated xorg-x11-server packages that fix various bugs are now available.

X.Org X11 is an open source implementation of the X Window System. It provides the basic low level functionality upon which graphical user interfaces such as GNOME and KDE are designed.

These updated packages address the following bugs:

\* resizing a glxgears window horizontally across the screen caused X to segfault. Changes were made in the related mesa packages and resizing no longer causes the error. ([BZ#435963](https://bugzilla.redhat.com/show_bug.cgi?id=435963)<sup>2215</sup>)

Note: due to the unusual build process for this package, the code fix is applied to the mesa packages, but the resulting compiled code is in the xorg-x11-server package (see [BZ#536868](https://bugzilla.redhat.com/show_bug.cgi?id=536868)<sup>2216</sup> for the bug as raised against mesa).

\* the X server ceased support for Pluggable Authentication Modules (PAM). Support for PAM was added back to the package and PAM can now be used as expected. ([BZ#486120](https://bugzilla.redhat.com/show_bug.cgi?id=486120)<sup>2217</sup>)

\* a patch had been added to the xorg-x11-server package which was going to cause compatibility issues between the xorg-x11-server package and proposed NVIDIA drivers. The randr-disabled-fb.patch was removed and the package should now work as expected. ([BZ#496108](https://bugzilla.redhat.com/show_bug.cgi?id=496108)<sup>2218</sup>)

\* the MGA and Xserver drivers were defaulting to inappropriate resolutions, causing the screen to go black, or be otherwise unreadable. The default values were changed, and resolution is now set to more reasonable values. ([BZ#507536](https://bugzilla.redhat.com/show_bug.cgi?id=507536)<sup>2219</sup> and [BZ#497853](https://bugzilla.redhat.com/show_bug.cgi?id=497853)<sup>2220</sup>)

\* when using multiple outputs on some ATI hardware, the GNOME screensaver and some related functions were not operating correctly. Changes were made to the xorg-x11-server package to better support the gnome-screensaver and xinerama functions and the screensaver now works correctly. ([BZ#516204](https://bugzilla.redhat.com/show_bug.cgi?id=516204)<sup>2221</sup>,

[BZ#530309](https://bugzilla.redhat.com/show_bug.cgi?id=530309)<sup>2222</sup> and [BZ#554571](https://bugzilla.redhat.com/show_bug.cgi?id=554571)<sup>2223</sup>)

---

<sup>2214</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=537759](https://bugzilla.redhat.com/show_bug.cgi?id=537759)

<sup>2215</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=435963](https://bugzilla.redhat.com/show_bug.cgi?id=435963)

<sup>2216</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=536868](https://bugzilla.redhat.com/show_bug.cgi?id=536868)

<sup>2217</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=486120](https://bugzilla.redhat.com/show_bug.cgi?id=486120)

<sup>2218</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=496108](https://bugzilla.redhat.com/show_bug.cgi?id=496108)

<sup>2219</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=507536](https://bugzilla.redhat.com/show_bug.cgi?id=507536)

<sup>2220</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=497853](https://bugzilla.redhat.com/show_bug.cgi?id=497853)

<sup>2221</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=516204](https://bugzilla.redhat.com/show_bug.cgi?id=516204)

<sup>2222</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=530309](https://bugzilla.redhat.com/show_bug.cgi?id=530309)

<sup>2223</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=554571](https://bugzilla.redhat.com/show_bug.cgi?id=554571)

\* changing to a higher resolution on Radeon 3100 hardware caused unexpected results on the desktop image. The X server resizing code was fixed to also resize the screen pixmap, and changing resolutions now works as expected. ([BZ#515609](#)<sup>2224</sup>)

\* the Anaconda graphical installer failed to start at the default 800x600 resolution on systems utilizing Intel Graphics Device Next Generation (IGDNG) devices. Support for this device has now been added, and Anaconda now starts correctly. ([BZ#510120](#)<sup>2225</sup>)

\* the X server did not automatically detect the QXL virtual graphics device, causing unexpected behavior with mouse detection and movement. The QXL driver is now loaded correctly and the mouse problems no longer manifest. ([BZ#558611](#)<sup>2226</sup>)

Users are advised to upgrade to these updated xorg-x11-server packages, which resolve these issues.

## 1.230. xorg-x11-xdm

### 1.230.1. RHBA-2009:1653: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTTRACK errata [RHBA-2009:1653](#)<sup>2227</sup>

An updated xorg-x11-xdm package that fixes a bug is now available.

xorg-x11-xdm provides a legacy display login manager for the X Window System.

This updated xorg-x11-xdm package fixes the following bug:

\* the xorg-x11-xdm package contained two PAM (Pluggable Authentication Modules) configuration files: "xdm" and "xserver". Because the xorg-x11-xdm package only requires the use of the "xdm" PAM configuration file, this update removes the second, spurious and unused PAM configuration file from the xorg-x11-xdm package. ([BZ#506535](#)<sup>2228</sup>)

All users of xorg-x11-xdm are advised to upgrade to this updated package, which resolves this issue.

## 1.231. xterm

### 1.231.1. RHBA-2009:1611: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as errata [RHBA-2009:1611](#)<sup>2229</sup>

<sup>2224</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=515609](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=515609)

<sup>2225</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=510120](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=510120)

<sup>2226</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=558611](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=558611)

<sup>2228</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=506535](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=506535)

An updated xterm package that fixes a bug is now available.

The xterm program is a terminal emulator for the X Window System. It provides DEC VT102 and Tektronix 4014 compatible terminals for programs that cannot use the window system directly.

This updated package includes the following bug fix:

\* missing pointer checks could cause xterm to SEGFAULT when the xterm window was resized during initialization. Pointer checking has been improved with this update and resizing an xterm window during initialization no longer causes xterm to crash. ([BZ#540534](#)<sup>2230</sup>)

All xterm users should upgrade to this updated package, which resolves this issue.

## 1.232. yaboot

### 1.232.1. RHBA-2010:0316: bug fix and enhancement update

An updated yaboot package that fixes a bug and adds an enhancement is now available.

The yaboot package is a boot loader for Open Firmware based PowerPC systems. It can be used to boot IBM eServer System p machines.

This updated package fixes the following bug:

\* previously the ybin binary returned exit code 1 even if there was no error message on output. (ybin returned exit code 0 if "ybin --verbose" was run with the same config file.) With this update ybin now returns exit code 0 when there is no output error message, as expected. ([BZ#515778](#)<sup>2231</sup>)

This update also adds the following enhancement:

\* the initrd chunksize was reduced for this update. This change allows yaboot to support init ram disks larger than 8192kB. ([BZ#562956](#)<sup>2232</sup>)

Note: previously, if yaboot attempted to use an initrd image larger than 8192 kB, booting failed with an "RAMDISK: ran out of compressed data" error message. Once this updated yaboot package is installed, using larger initrd images with yaboot will work as expected.

All PowerPC yaboot users are advised to upgrade to this updated package, which resolves this issue and adds this enhancement.

## 1.233. yp-tools

### 1.233.1. RHBA-2009:1609: bug fix update



#### Note

This update has already been released (prior to the GA of this release) as FASTRACK errata [RHBA-2009:1609](#)<sup>2233</sup>

---

<sup>2230</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=540534](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=540534)

<sup>2231</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=515778](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=515778)

<sup>2232</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=562956](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=562956)

Updated yp-tools packages that fix a bug are now available.

The Network Information Service (NIS) is a system which provides network information (login names, passwords, home directories, group information) to all of the machines on a network. NIS can enable users to login on any machine on the network, as long as the machine has the NIS client programs running and the user's password is recorded in the NIS passwd database. NIS was formerly known as Sun Yellow Pages (YP).

These updated yp-tools packages fix the following bug:

\* the yp-tools-debuginfo package did not contain debugging information, even though the yp-tools package itself contained ELF (Executable and Linking Format) objects. With these updated packages, the debuginfo package now contains debugging information. ([BZ#500642](#)<sup>2234</sup>)

All users of yp-tools are advised to upgrade to these updated packages, which resolve this issue.

## 1.234. yum

### 1.234.1. RHBA-2010:0254: bug fix update

An updated yum package that fixes various bugs is now available.

Yum is a utility that can check for and automatically download and install updated RPM packages. Dependencies are obtained and downloaded automatically, prompting the user for permission as necessary.

Bugs fixed in these updated packages include:

- \* fix bugtracker URL. ([BZ#528738](#)<sup>2235</sup>)
- \* fix return code error during 'yum reinstall'. ([BZ#528746](#)<sup>2236</sup>)
- \* remove slow edge case from compare\_providers. ([BZ#529233](#)<sup>2237</sup>)
- \* add base package name check to compare\_providers(). ([BZ#529719](#)<sup>2238</sup>)
- \* fix instant downloads crash. ([BZ#517286](#)<sup>2239</sup>)
- \* fix exit regression when updating packages that do not exist. ([BZ#521008](#)<sup>2240</sup>)
- \* show obsoletes in check-update, if obsoletes flag is on. ([BZ#526064](#)<sup>2241</sup>)

All yum users should upgrade to this updated package, which resolves these issues.

---

<sup>2234</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=500642](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=500642)

<sup>2235</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=528738](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=528738)

<sup>2236</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=528746](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=528746)

<sup>2237</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=529233](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=529233)

<sup>2238</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=529719](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=529719)

<sup>2239</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=517286](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=517286)

<sup>2240</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=521008](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=521008)

<sup>2241</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=526064](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=526064)

### 1.235. yum-rhn-plugin

#### 1.235.1. RHBA-2010:0269: bug fix and enhancement update

An updated yum-rhn-plugin package that fixes several bugs and provides new functionality is now available.

yum-rhn-plugin allows yum to access a Red Hat Network server for software updates.

This update fixes several bugs and implements new features:

- \* ability to permanently enable and disable yum repositories provided by RHN / RHN Satellite via pirut tool. ([BZ#437822](https://bugzilla.redhat.com/show_bug.cgi?id=437822)<sup>2242</sup>)
- \* remove unnecessary debug information printed by yum when run in silent mode ([BZ#504295](https://bugzilla.redhat.com/show_bug.cgi?id=504295)<sup>2243</sup>)
- \* stock rhnplugin.conf now contains examples of configuration options for repositories provided by RHN / RHN Satellite. ([BZ#509342](https://bugzilla.redhat.com/show_bug.cgi?id=509342)<sup>2244</sup>)
- \* disable yum repositories provided by RHN / RHN Satellite in case /etc/sysconfig/rhn/systemid was removed. ([BZ#514467](https://bugzilla.redhat.com/show_bug.cgi?id=514467)<sup>2245</sup>)
- \* require recent version of rhn-client-tools package to avoid a traceback when invoking 'yum clean all' command. (BZ #515575)
- \* correctly rollback to older version of a package in scenarios where the package was split in later versions. (BZ #524237)
- \* correctly update log files when performing package updates and removals from RHN / RHN Satellite. (BZ #527412)

Users of yum-rhn-plugin are advised to upgrade to this updated package, which fixes these issues.

---

<sup>2242</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=437822](https://bugzilla.redhat.com/show_bug.cgi?id=437822)

<sup>2243</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=504295](https://bugzilla.redhat.com/show_bug.cgi?id=504295)

<sup>2244</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=509342](https://bugzilla.redhat.com/show_bug.cgi?id=509342)

<sup>2245</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=514467](https://bugzilla.redhat.com/show_bug.cgi?id=514467)



# New Packages

## New Packages

### 2.1. RHEA-2010:0305: freeradius2

A new package, freeradius2, is now available.

FreeRADIUS is an Internet authentication daemon, which implements the RADIUS protocol, as defined in RFC 2865 (and others). It allows Network Access Servers (NAS boxes) to perform authentication for dial-up users. There are also RADIUS clients available for Web servers, firewalls, Unix logins, and more. Using RADIUS allows authentication and authorization for a network to be centralized, and minimizes the amount of re-configuration which has to be done when adding or deleting new users.

Red Hat Enterprise Linux 5 originally shipped with FreeRADIUS 1.1.3. Since that time the FreeRADIUS project has had a major new release: FreeRADIUS 2. Because of the numerous enhancements available in FreeRADIUS 2 many users would prefer to use the more contemporary version of FreeRADIUS. This new package, provides this newer version. ([BZ#473704](#)<sup>1</sup>)

Note: versions 1.x and 2.x of FreeRADIUS are not configuration compatible. Red Hat will continue to support and make available freeradius-1.1.3. Customers who are utilizing the original freeradius-1.1.3 will see no difference. For customers who wish to utilize the newer 2.x version of FreeRADIUS in Red Hat Enterprise Linux 5 the new freeradius2 package provides that capability.

Note: freeradius and freeradius2 cannot be installed simultaneously. Because they share common files, rpm, the Red Hat Enterprise Linux package manager, will prevent an installation of FreeRADIUS 2.x if FreeRADIUS 1.x is already installed. To install freeradius2 on a system with freeradius currently installed, freeradius must first be uninstalled. See the solution section below for details.

Users wanting to take advantage of the enhancements available in FreeRADIUS 2.x should install and configure this new package.

### 2.2. RHEA-2010:0240: gpXE

A new package, gPXEm, is now available for Red Hat Enterprise Linux 5.5

gPXEm is an open source Preboot Execution Environment (PXE) implementation and bootloader. Designed to be direct replacement for proprietary PXE ROMs, gPXEm also supports additional protocols such as DNS, HTTP, iSCSI and ATA over Ethernet. gPXEm is a significantly restructured update to the original Etherboot package.

Previously gPXEm was available as a separate, and not officially supported, ISO image. As part of the Red Hat Enterprise Linux 5.5 update, a gPXEm package containing ROMs for devices emulated by QEMU is now available as an integrated and supported Red Hat Enterprise Linux package. ([BZ#512045](#)<sup>2</sup> & [BZ#545886](#)<sup>3</sup>)

Note: gPXEm does not replace etherboot. Both packages, however, write their .zrom files to the same directory -- /usr/share/pxe-boot. KVM links to whatever ROM files are present in /usr/share/pxe-boot

---

<sup>1</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=473704](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=473704)

<sup>2</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=512045](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=512045)

<sup>3</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=545886](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=545886)

and installing gPXE provides support for several specific PXE servers that are not supported by Etherboot.

KVM users wanting PXE server support not provided by Etherboot should install this new package.

### 2.3. RHEA-2010:0199: gsl

The new package `gsl` is now available.

The GNU Scientific Library (GSL) is a collection of routines for numerical analysis, written in C.

The `gsl` package contains the header files and static libraries necessary for developing programs using the GSL.

Anyone wishing to take advantage of the numerical analysis tools provided by this package should install this new package.

### 2.4. RHEA-2010:0217: iwl1000-firmware

An `iwl1000-firmware` package that matches the `iwlagn` driver in the latest Red Hat Enterprise Linux kernels is now available.

The `iwlagn` driver supports the Intel Wireless WiFi Link 1000BGN services adapter. This driver requires firmware to be loaded onto a device in order to function on that device.

This new `iwl1000-firmware` package contains the firmware required by the `iwlagn` driver in order to support the Intel Wireless WiFi Link 1000BGN series adapter on Red Hat Enterprise Linux. ([BZ#519223](https://bugzilla.redhat.com/show_bug.cgi?id=519223)<sup>4</sup>)

Users of the `iwlagn` driver are advised to install this new package, which provides this enhancement.

### 2.5. RHEA-2010:0220: iwl6000-firmware

A new `iwl6000-firmware` package that works with the `iwlagn` driver in the latest Red Hat Enterprise Linux kernels to enable support for Intel Wireless WiFi Link 6000 Series AGN Adapters is now available.

`iwlagn` is a kernel driver module for the Intel Wireless WiFi Link 4965AGN, 5100AGN, 5300AGN, 5350AGN, 5150AGN, 1000BGN and 6000AGN series of devices. The `iwlagn` driver requires firmware loaded on the device in order to function.

This new `iwl6000-firmware` package provides the firmware required by `iwlagn` to enable Intel Wireless WiFi Link 6000 Series AGN Adapters (aka `iwl6000` devices). ([BZ#526292](https://bugzilla.redhat.com/show_bug.cgi?id=526292)<sup>5</sup>)

All users of the `iwlagn` driver, especially those requiring `iwl6000` support, should install this new package, which provides this enhancement.

### 2.6. RHEA-2010:0276: postgresql84

New `postgresql84` packages are now available.

---

<sup>4</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=519223](https://bugzilla.redhat.com/show_bug.cgi?id=519223)

<sup>5</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=526292](https://bugzilla.redhat.com/show_bug.cgi?id=526292)

PostgreSQL is an advanced object-relational database management system (DBMS) that supports almost all SQL constructs (including transactions, subselects and user-defined types and functions).

The postgresql84 packages provide the current 8.4.x release series of PostgreSQL, superseding the 8.1.x series originally shipped with Red Hat Enterprise Linux 5. Since there are many minor application-level incompatibilities between 8.1.x and 8.4.x, the original postgresql package set remains available and will continue to be updated.

postgresql84 is for those users who wish to migrate to a more current PostgreSQL release.

postgresql84 and postgresql packages cannot be installed concurrently on the same system, with the exception that the postgresql-libs package can remain in place in parallel with postgresql84. The postgresql-libs package contains client-side library code to which existing applications may be linked. These libraries will still work with the newer server.

As 8.4.x also has on-disk data format differences from 8.1.x, it is not possible to upgrade an existing 8.1.x PostgreSQL database to 8.4.x merely by replacing the packages. Instead, first dump the contents of the existing database using the `pg_dumpall` command, then shut down the old server and remove the database files (under `/var/lib/pgsql/data`). Next, remove the old packages and install the new ones; start the new server; and finally restore the data from the `pg_dumpall` output.

Note, there are two known issues with this new package as follows:

\* on Itanium, the only supported development subpackage architecture is Itanium. While it is possible to install both i386 and ia64 packages, these contain conflicting files and using the both architectures together may lead to unpredictable results. The i386 version is unsupported, as the Itanium version of gcc cannot compile code executable using the IA32 emulation capability. ([BZ#489479](https://bugzilla.redhat.com/show_bug.cgi?id=489479)<sup>6</sup>)

\* while postgresql84 packages are provided, rebuilding other packages with this new version is not supported. If a package using postgresql-devel is to be rebuilt, a downgrade from postgresql84 to postgresql is necessary. ([BZ#558746](https://bugzilla.redhat.com/show_bug.cgi?id=558746)<sup>7</sup>)

Subject to the limitations noted above, users wishing to run PostgreSQL 8.4.x are encouraged to install these new packages.

## 2.7. RHEA-2010:0268: python-dmidecode

A new package, python-dmidecode, is now available for Red Hat Enterprise Linux 5.

The python-dmidecode module is a Python extension that uses the code-base of the dmidecode utility, and presents the DMI data as Python dictionaries or XML utilizing libxml2.

The Desktop Management Interface (DMI) provides the infrastructure for x86-based systems to pass component-level information up to other applications. The dmidecode utility reads and reports the information as presented in the DMI tables by a system's BIOS. By providing this data as Python dictionaries or XML, the new python-dmi-decode module makes this information available to Python-based applications or applications that can parse XML. ([BZ#546220](https://bugzilla.redhat.com/show_bug.cgi?id=546220)<sup>8</sup>)

Note: PowerPC and IBM System z systems do not use the DMI standard and, consequently, do not have DMI tables to decode. If the python-dmidecode module is installed on these systems, however, the module can read supplied DMI data from x86-based systems.

<sup>6</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=489479](https://bugzilla.redhat.com/show_bug.cgi?id=489479)

<sup>7</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=558746](https://bugzilla.redhat.com/show_bug.cgi?id=558746)

<sup>8</sup> [https://bugzilla.redhat.com/show\\_bug.cgi?id=546220](https://bugzilla.redhat.com/show_bug.cgi?id=546220)

x86-based systems users wanting to access DMI table data with Python- or XML-based tools should install this new package which provides this capability.

### 2.8. RHEA-2010:0249: tunctl

A new package, tunctl, is now available for Red Hat Enterprise Linux 5.

tunctl is a tool to set up and maintain persistent Network Tunnel and Network Tap (TUN/TAP) interfaces, enabling user applications access to the wire side of a virtual network interface. Such interfaces are useful for connecting VPN software, virtualization, emulation and a number of other similar applications to the network stack.

\* using tunctl a system administrator can create, configure and manage persistent TUN/TAP interfaces for use by a designated user or group. This particular user or group can then open and use the network-facing interface but can not alter any aspect of the host side of the interface. ([BZ#501574](#)<sup>9</sup>)

Administrators wanting to enable persistent TUN/TAP interfaces and manage access to these interfaces by uid, gid or both should install this new package.

### 2.9. RHEA-2010:0189: xz

A new package, xz, which provides user-space tools for compressing and decompressing files with the LZMA algorithm, is now available.

XZ Utils is an integrated collection of user-space file compression utilities based on the Lempel-Ziv-Markov chain-Algorithm (LZMA) compression algorithm. LZMA is a general purpose compression algorithm designed by Igor Pavlov as part of 7-Zip. It provides high compression ratio while keeping decompression times low.

The xz package includes liblzma, an LZMA library and API; xz, a shell tool for compressing files; and xzdec, a shell tool for de-compressing files. The liblzma API is similar to zlib's and the behavior of xz and xzdec will be familiar to users of gzip. Also, .xz files have similar properties to files produced by gzip and bzip2, making them easy for users familiar with these tools to work with. The LZMA algorithm, however, provides generally better compression ratios than these conventional tools. ([BZ#519122](#)<sup>10</sup>)

Anyone interested in taking advantage of this new compression utility should install this new package.

---

<sup>9</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=501574](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=501574)

<sup>10</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=519122](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=519122)

## Technology Previews

*Technology Preview* features are currently *not* supported under Red Hat Enterprise Linux subscription services, may not be functionally complete, and are generally not suitable for production use. However, these features are included as a customer convenience and to provide the feature with wider exposure.

Customers may find these features useful in a non-production environment. Customers are also free to provide feedback and functionality suggestions for a Technology Preview feature before it becomes fully supported. Erratas will be provided for high-severity security issues.

During the development of a Technology Preview feature, additional components may become available to the public for testing. It is the intention of Red Hat to fully support Technology Preview features in a future release.

### Brocade BFA Fibre-Channel/FCoE driver

the **bfa** driver for Brocade Fibre Channel Host Bus adapters has been added to Red Hat Enterprise Linux 5.5 as a Technology Preview. [BZ#475695](#)<sup>1</sup>

### ext4

The latest generation of the ext filesystem, **ext4**, is available in this release as a Technology Preview. **Ext4** is an incremental improvement on the **ext3** file system developed by Red Hat and the Linux community. The release name of the file system for the Technology Preview is **ext4dev**.

The file system is provided by the **ext4dev.ko** kernel module, and a new **e4fsprogs** package, which contains updated versions of the familiar e2fsprogs administrative tools for use with ext4. To use, install **e4fsprogs** and then use commands like **mkfs.ext4dev** from the e4fsprogs program to create an ext4-base file system. When referring to the filesystem on a mount commandline or fstab file, use the filesystem name **ext4dev**.

### FreeIPMI

*FreeIPMI* is now included in this update as a Technology Preview. FreeIPMI is a collection of Intelligent Platform Management IPMI system software. It provides in-band and out-of-band software, along with a development library conforming to the Intelligent Platform Management Interface (IPMI v1.5 and v2.0) standards.

For more information about FreeIPMI, refer to <http://www.gnu.org/software/freeipmi/>

### TrouSerS and tpm-tools

*TrouSerS* and **tpm-tools** are included in this release to enable use of *Trusted Platform Module* (TPM) hardware. TPM hardware features include (among others):

- Creation, storage, and use of RSA keys securely (without being exposed in memory)
- Verification of a platform's software state using cryptographic hashes

*TrouSerS* is an implementation of the Trusted Computing Group's Software Stack (TSS) specification. You can use *TrouSerS* to write applications that make use of TPM hardware. **tpm-tools** is a suite of tools used to manage and utilize TPM hardware.

For more information about *TrouSerS*, refer to <http://trousers.sourceforge.net/>.

---

<sup>1</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=475695](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=475695)

### eCryptfs

**eCryptfs** is a stacked cryptographic file system for Linux. It mounts on individual directories in existing mounted lower file systems such as EXT3; there is no need to change existing partitions or file systems in order to start using **eCryptfs**.

With this release, **eCryptfs** has been re-based to upstream version 56, which provides several bug fixes and enhancements. In addition, this update provides a graphical program to help configure **eCryptfs** (`ecryptfs-mount-helper-gui`).

This update also changes the syntax of certain **eCryptfs** mount options. If you choose to update to this version of **eCryptfs**, you should update any affected mount scripts and `/etc/fstab` entries. For information about these changes, refer to `man ecryptfs`.

The following caveats apply to this release of **eCryptfs**:

- Note that the **eCryptfs** file system will only work properly if the encrypted file system is mounted once over the underlying directory of the same name. For example:

```
mount --t ecryptfs -/mnt/secret -/mnt/secret
```

The secured portion of the file system should not be exposed, i.e. it should not be mounted to other mount points, bind mounts, and the like.

- **eCryptfs** mounts on networked file systems (e.g. NFS, Samba) will not work properly.
- This version of the **eCryptfs** kernel driver requires updated userspace, which is provided by `ecryptfs-utils-56-4.el5` or newer.

For more information about **eCryptfs**, refer to <http://ecryptfs.sf.net>. You can also refer to <http://ecryptfs.sourceforge.net/README> and <http://ecryptfs.sourceforge.net/ecryptfs-faq.html> for basic setup information.

### Stateless Linux

Stateless Linux is a new way of thinking about how a system should be run and managed, designed to simplify provisioning and management of large numbers of systems by making them easily replaceable. This is accomplished primarily by establishing prepared system images which get replicated and managed across a large number of stateless systems, running the operating system in a read-only manner (refer to `/etc/sysconfig/readonly-root` for more details).

In its current state of development, the Stateless features are subsets of the intended goals. As such, the capability remains as Technology Preview.

Red Hat recommends that those interested in testing stateless code read the HOWTO at <http://fedoraproject.org/wiki/StatelessLinux/HOWTO> and join [stateless-list@redhat.com](mailto:stateless-list@redhat.com)<sup>8</sup>.

The enabling infrastructure pieces for Stateless Linux were originally introduced in Red Hat Enterprise Linux 5.

### AIGLX

**AIGLX** is a Technology Preview feature of the otherwise fully supported X server. It aims to enable GL-accelerated effects on a standard desktop. The project consists of the following:

- A lightly modified X server.

---

<sup>8</sup> <mailto:stateless-list@redhat.com>

- 
- An updated Mesa package that adds new protocol support.

By installing these components, you can have GL-accelerated effects on your desktop with very few changes, as well as the ability to enable and disable them at will without replacing your X server. AIGLX also enables remote GLX applications to take advantage of hardware GLX acceleration.

#### FireWire

The **firewire-sbp2** module is still included in this update as a Technology Preview. This module enables connectivity with FireWire storage devices and scanners.

At present, FireWire does not support the following:

- IPv4
- *pcilynx* host controllers
- multi-LUN storage devices
- non-exclusive access to storage devices

In addition, the following issues still exist in FireWire:

- a memory leak in the **SBP2** driver may cause the machine to become unresponsive.
- a code in this version does not work properly in big-endian machines. This could lead to unexpected behavior in PowerPC.

#### ktune

This release includes **ktune** (from the **ktune** package), a service that sets several kernel tuning parameters to values suitable for specific system profiles. Currently, **ktune** only provides a profile for large-memory systems running disk-intensive and network-intensive applications.

The settings provided by **ktune** do not override those set in `/etc/sysctl.conf` or through the kernel command line. **ktune** may not be suitable on some systems and workloads; as such, you should test it comprehensively before deploying to production.

You can disable any configuration set by **ktune** and revert to your normal settings by simply stopping the **ktune** service using `service ktune stop` (as root).

#### SGPIO Support for dmraid

Serial General Purpose Input Output (SGPIO) is an industry standard communication method used between a main board and a variety of internal and external hard disk drive bay enclosures. This method can be used to control LED lights on an enclosure through the AHCI driver interface.

In this release, SGPIO support in **dmraid** is included as a technology preview. This will allow **dmraid** to work properly with disk enclosures.

#### GCC 4.4

The *Gnu Compiler Collection version 4.4 (GCC4.4)* is now included in this release as a Technology Preview. This collection of compilers includes C, C++, and Fortran compilers along with support libraries.

Note that in the **gcc44** packages, the default for the **gnu89-inline** option has been changed to **-fgnu89-inline**, whereas upstream and future updates of Red Hat Enterprise Linux 5 will



default to **-fno-gnu89-inline**. This is necessary because many headers shipped as part of Red Hat Enterprise Linux 5 expect GNU in-line semantics instead of ISO C99 semantics. These headers have not been adjusted to request GNU in-line semantics through attributes.

### Kernel Tracepoint Facility

In this update, a new kernel marker/tracepoint facility has been implemented as a Technology Preview. This interface adds static probe points into the kernel, for use with tools such as **SystemTap**.

### Device Failure Monitoring of RAID sets

Device Failure Monitoring, using the tools `dmraid` and `dmevent_tool`, is included in Red Hat Enterprise Linux 5.5 as a Technology Preview. This provides the ability to watch and report device failures on component devices of RAID sets.

### Software based Fibre Channel over Ethernet (FCoE)

The Fibre Channel over Ethernet (FCoE) driver (`fcoe.ko`), along with `libfc`, provides the ability to run FCoE over a standard Ethernet card. This capability is provided as a technical preview in Red Hat Enterprise Linux 5.5.

To enable this feature, you must login by writing the network interface name to the `/sys/module/fcoe/parameters/create` file, for example:

```
echo eth6 > /sys/module/fcoe/parameters/create
```

To logout, write the network interface name to the `/sys/module/fcoe/parameters/destroy` file, for example:

```
echo eth6 > /sys/module/fcoe/parameters/destroy
```

For further information on software based FCoE refer to: [http://www.open-fcoe.org/openfc/wiki/index.php/FCoE\\_Initiator\\_Quickstart](http://www.open-fcoe.org/openfc/wiki/index.php/FCoE_Initiator_Quickstart).

Red Hat Enterprise Linux 5.5 provides full support for FCoE on three specialized hardware implementations. These are: Cisco **fnic** driver, the Emulex **lpfc** driver, and the Qlogic **qla2xx** driver.

### iSER Support

iSER support, allowing for block storage transfer across a network, has been added to the **scsi-target-utils** package as a Technology Preview. In this release, single portal and multiple portals on different subnets are supported. There are known bugs when using multiple portals on the same subnet.

To set up the iSER target component install the `scsi-target-utils` and `libibverbs-devel` RPM. The library package for the InfiniBand hardware that is being used is also required. For example: host channel adapters that use the **cxgb3** driver the **libcxgb3** package is needed, and for host channel adapters using the **mtcha** driver the **libmtcha** package is needed.

There is also a known issue relating to connection timeouts in some situations. Refer to [Red Hat Bugzilla #470627](#)<sup>19</sup> for more information on this issue.

---

<sup>19</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=470627](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=470627)

---

## iSER Support

iSER support, allowing for block storage transfer across a network, has been added to the **scsi-target-utils** package as a Technology Preview. In this release, single portal and multiple portals on different subnets are supported. There are known bugs when using multiple portals on the same subnet.

To set up the iSER target component install the `scsi-target-utils` and `libibverbs-devel` RPM. The library package for the InfiniBand hardware that is being used is also required. For example: host channel adapters that use the **cxgb3** driver the **libcxgb3** package is needed, and for host channel adapters using the **mtl** driver the **libmtl** package is needed.

There is also a known issue relating to connection timeouts in some situations. Refer to [Red Hat Bugzilla #470627](#)<sup>21</sup> for more information on this issue.

## cman fence\_virsh fence agent

The `fence_virsh` fence agent is provided in this release of Red Hat Enterprise Linux as a Technology Preview. `fence_virsh` provides the ability for one guest (running as a domU) to fence another using the libvirt protocol. However, as `fence_virsh` is not integrated with `cluster-suite` it is not supported as a fence agent in that environment.

## glibc new MALLOC behaviour

The upstream glibc has been changed recently to enable higher scalability across many sockets and cores. This is done by assigning threads their own memory pools and by avoiding locking in some situations. The amount of additional memory used for the memory pools (if any) can be controlled using the environment variables `MALLOC_ARENA_TEST` and `MALLOC_ARENA_MAX`.

`MALLOC_ARENA_TEST` specifies that a test for the number of cores is performed once the number of memory pools reaches this value. `MALLOC_ARENA_MAX` sets the maximum number of memory pools used, regardless of the number of cores.

The glibc in the Red Hat Enterprise Linux 5.5 release has this functionality integrated as a Technology Preview of the upstream malloc. To enable the per-thread memory pools the environment variable `MALLOC_PER_THREAD` needs to be set in the environment. This environment variable will become obsolete when this new malloc behaviour becomes default in future releases. Users experiencing contention for the malloc resources could try enabling this option.

---

<sup>21</sup> [https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=470627](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=470627)

---

# Capabilities and Limits

This chapter documents the capabilities and limits of Red Hat Enterprise Linux 5 as of minor release Red Hat Enterprise Linux 5.5.

Red Hat maintains a technology capabilities and limits page for Red Hat Enterprise Linux at <http://www.redhat.com/rhel/compare/>. This page provides the theoretical limits supported by the software as well as certified limits for generally available hardware. The theoretical limits are updated with every major release. Certified limits reflect the current state of system testing by Red Hat and its partners for mainstream hardware.



## Note

All the certified limits documented in this section are current as of March 30th 2010.

### Maximum Logical CPUs

Logical CPU is defined as the number of CPUs that are presented to the operating system by the hardware. Multi-core processors and hyperthreads increase the number of logical CPUs that are visible to the operating system.

	Certified
x86	32
Itanium2	256
AMD64/Intel64	64
Power	128
System z	64 (z10 EC)

### Maximum memory

	Certified
x86	16GB
Itanium2	2TB
AMD64/Intel64	256GB
Power	512GB
System z	1.5TB (z10 EC)



# Known Issues

## 5.1. anaconda

The anaconda package contains the program which was used to install your system.

The following are the Known Issues that apply to the anaconda package in Red Hat Enterprise Linux 5

- anaconda sometimes crashes while attempting to install on a disk containing partitions or filesystems used by other operating systems. To work around this issue, clear the existing partition table using the command:

```
clearpart ---initlabel [disks]
```

[BZ#530465](#)<sup>1</sup>

- Performing a System z installation when the install.img is located on direct access storage device (DASD) disk, will cause the installer to crash, returning a backtrace. anaconda is attempting to re-write (commit) all disk labels when partitioning is complete, but is failing because the partition is busy. To work around this issue, a non-DASD source should be used for install.img. [BZ#455929](#)<sup>2</sup>
- When installing to an ext3 or ext4 file system, anaconda disables periodic filesystem checking. Unlike ext2, these filesystems are journaled, removing the need for a periodic filesystem check. In the rare cases where there is an error detected at runtime or an error while recovering the filesystem journal, the file system check will be run at boot time. ([BZ#513480](#))<sup>3</sup>
- If unmodified kickstart files from Red Hat Enterprise Linux 5.4 are used to install Red Hat Enterprise Linux 5.5, anaconda may crash and complain that the directory required to save the log files does not exist. ([BZ#568861](#))<sup>4</sup>
- Red Hat Enterprise Linux 5 does not support having a separate /var on a network filesystem (nfs, iscsi disk, nbd, etc.) This is because /var contains the utilities required to bring up the network, for example /var/lib/dhcp. However, you may have /var/spool, /var/www or the like on a separate network disk, just not the complete /var filesystem. [BZ#485478](#)<sup>5</sup>
- When using rescue mode on an installation which uses iscsi drives which were manually configured during installation, the automatic mounting of the root filesystem will not work and you need to configure iscsi and mount the filesystems manually. This only applies to manual configured iscsi drives, iscsi drives which are automatically detected through ibft are fully supported in rescue mode.

To rescue a system which has / on a non ibft configured iscsi drive, choose to skip the mounting of the root fs when asked and then follow the steps below.

```
$TARGET_IP: IP address of the iscsi target (drive)
$TARGET_IQN: name of the iscsi target as printed by the discovery command
$ROOT_DEV: devicenode (/dev/.....) where your root fs lives
```

1. Define an initiator name.

```
$ mkdir -/etc/iscsi
```

```
$ cat << EOF>> /etc/iscsi/initiatorname.iscsi
InitiatorName=iqn.1994-05.com.fedora:d62f2d7c09f
EOF
```

### 2. Start iscsid

```
$ iscsid
```

### 3. Discover and login to target:

```
$ iscsiadm --m discovery --t st --p $TARGET_IP
$ iscsiadm --m node --T $TARGET_IQN --p $TARGET_IP ---login
```

### 4. If the iSCSI LUN is part of a LVM Logical volume group

```
$ lvm vgscan
$ lvm vgchange --ay
```

### 5. Now mount your '/' partition

```
$ mount -/dev/path/to/root -/mnt/sysimage
$ mount --t bind -/dev -/mnt/sysimage/dev
$ mount --t proc proc -/mnt/sysimage/proc
$ mount --t sysfs sysfs -/mnt/sysimage/sys
```

### 6. Now you can chroot to the root fs of your installation if wanted

```
$ chroot -/mnt/sysimage -/bin/su --
```

([BZ#248022](#))<sup>6</sup>

- When installing KVM or Xen guests, always create a partition for the guest disk, or create an LVM volume. Guests should not be installed to block devices or raw disk devices. Anaconda includes disk label duplication avoidance code, but when installing within a VM, it has no visibility to the disk labels elsewhere on the host and cannot detect duplicates.

If guest filesystems, especially the root filesystem, are directly visible to the host, a host OS reboot may inadvertently parse the partition table and mount the guest filesystems. This can lead to highly undesirable outcomes. ([BZ#518461](#))<sup>7</sup>

- The minimum memory requirement when installing all Red Hat Enterprise Linux packages (i.e. '\*' or '@everything' is listed in the %packages section of the kickstart file) on a fully virtualized Itanium guest is 768MB. After installation, the memory allocated to the guest can be lowered to the desired amount. ([BZ#507891](#))<sup>8</sup>
- Upgrading a system using Anaconda is not possible if the system is installed on disks attached using zFCP or iSCSI (unless booted from the disk using a network adaptor with iBFT). Such disks are activated after Anaconda scans for upgradable installations and are not found. To update please



use the Red Hat Network with the hosted Web user interface, a Red Hat Network Satellite, the local graphical Updater, or the yum command line. (BZ#494033)<sup>9</sup>

- Anaconda's graphical installer fails to start at the default 800x600 resolution on systems utilizing Intel Graphics Device Next Generation (IGDNG) devices. To work around this issue, ensure anaconda uses a higher resolution by passing the parameters **resolution=1024x768** or **resolution=1280x1024** to the installer using the boot command line.
- The NFS default for RHEL5 is "locking". Therefore, to mount nfs shares from the %post section of anaconda, use the **mount -o nolock,udp** command to start the locking daemon before using nfs to mount shares. (BZ#426053)<sup>10</sup>
- If you are using the Virtualized kernel when upgrading from Red Hat Enterprise Linux 5.0 to a later 5.x release, you must reboot after completing the upgrade. You should then boot the system using the updated Virtualized kernel.

The hypervisor ABI changes in an incompatible way between Red Hat Enterprise Linux 5 and 5.1. If you do not boot the system after upgrading from RHEL 5.0 using the updated Virtualized kernel, the upgraded Virtualization RPMs will not match the running kernel. (BZ#251669)<sup>11</sup>

- When upgrading from Red Hat Enterprise Linux 4.6 to Red Hat Enterprise Linux 5.1 or later, gcc4 may cause the upgrade to fail. As such, you should manually remove the gcc4 package before upgrading. (BZ#432773)<sup>12</sup>
- When provisioning guests during installation, the **RHN tools for guests** option will not be available. When this occurs, the system will require an additional entitlement, separate from the entitlement used by **dom0**.

To prevent the consumption of additional entitlements for guests, install the **rhn-virtualization-common** package manually before attempting to register the system to Red Hat Network. (BZ#431648)<sup>13</sup>

- When installing Red Hat Enterprise Linux 5 on a guest, the guest is configured to explicitly use a temporary installation kernel provided by **dom0**. Once installation finishes, it can then use its own bootloader. However, this can only be achieved by forcing the guest's first reboot to be a shutdown.

As such, when the **Reboot** button appears at the end of the guest installation, clicking it shuts down the guest, but does not reboot it. This is an expected behavior.

Note that when you boot the guest after this it will then use its own bootloader. (BZ#328471)<sup>14</sup>

- Using the **swap --grow** parameter in a kickstart file without setting the **--maxsize** parameter at the same time makes anaconda impose a restriction on the maximum size of the swap partition. It does not allow it to grow to fill the device.

For systems with less than 2GB of physical memory, the imposed limit is twice the amount of physical memory. For systems with more than 2GB, the imposed limit is the size of physical memory plus 2GB. (BZ#462734)<sup>15</sup>

- Existing encrypted block devices that contain **vfat** file systems will appear as type **foreign** in the partitioning interface; as such, these devices will not be mounted automatically during system boot. To ensure that such devices are mounted automatically, add an appropriate entry for them to **/etc/fstab**. For details on how to do so, refer to **man fstab**. (BZ#467202)<sup>16</sup>

- when using anaconda's automatic partitioning on an IBM System p partition with multiple harddisks containing different Linux distributions, the anaconda installer may overwrite the bootloaders of the other Linux installations although their harddisks have been unchecked. To work around this, choose manual partitioning during the installation process. [\(BZ#519795\)](#)<sup>17</sup>

The following note applies to PowerPC Architectures:

- The minimum RAM required to install Red Hat Enterprise Linux 5.2 is 1GB; the recommended RAM is 2GB. If a machine has less than 1GB RAM, the installation process may hang.

Further, PowerPC-based machines that have only 1GB of RAM experience significant performance issues under certain RAM-intensive workloads. For a Red Hat Enterprise Linux 5.2 system to perform RAM-intensive processes optimally, 4GB of RAM is recommended. This ensures the system has the same number of physical pages as was available on PowerPC machines with 512MB of RAM running Red Hat Enterprise Linux 4.5 or earlier. [\(BZ#209165\)](#)<sup>18</sup>

The following note applies to s390x Architectures:

- Installation on a machine with existing Linux or non-Linux filesystems on DASD block devices may cause the installer to halt. If this happens, it is necessary to clear out all existing partitions on the DASD devices you want to use and restart the installer. [\(BZ#289631\)](#)<sup>19</sup>

The following note applies to the ia64 Architecture:

- If your system only has 512MB of RAM, attempting to install Red Hat Enterprise Linux 5.4 may fail. To prevent this, perform a base installation first and install all other packages after the installation finishes. [\(BZ#435271\)](#)<sup>20</sup>

## 5.2. cmirror

The cmirror packages provide user-level utilities for managing cluster mirroring.

- Due to limitations in the cluster infrastructure, cluster mirrors greater than 1.5TB cannot be created with the default region size. If larger mirrors are required, the region size should be increased from its default (512kB), for example:

```
# --R <region_size_in_MiB>
lvcreate --m1 --L 2T --R 2 --n mirror vol_group
```

Failure to increase the region size will result in the LVM creation process hanging and may cause other LVM commands to hang. [\(BZ#514814\)](#)<sup>21</sup>

## 5.3. compiz

Compiz is an OpenGL-based window and compositing manager.

- Running **rpmbuild** on the **compiz** source RPM will fail if any KDE or **qt** development packages (for example, **qt-devel**) are installed. This is caused by a bug in the **compiz** configuration script.

To work around this, remove any KDE or **qt** development packages before attempting to build the **compiz** package from its source RPM. [\(BZ#444609\)](#)<sup>22</sup>

## 5.4. ctdb

CTDB is a clustered database based on Samba's Trivial Database (TDB). The ctdb package is a cluster implementation used to store temporary data. If an application is already using TDB for temporary data storage, it can be very easily converted to be cluster-aware and use CTDB.

- When installing ctdb, the tdb-tools package needs to be installed manually. This dependency issues will be addressed in a future release. ([BZ#526479](#)<sup>23</sup>)

## 5.5. device-mapper-multipath

The device-mapper-multipath packages provide tools to manage multipath devices using the device-mapper multipath kernel module.

- When using **dm-multipath**, if **features "1 queue\_if\_no\_path"** is specified in **/etc/multipath.conf** then any process that issues I/O will hang until one or more paths are restored.

To avoid this, set **no\_path\_retry [N]** in **/etc/multipath.conf** (where **[N]** is the number of times the system should retry a path). When you do, remove the **features "1 queue\_if\_no\_path"** option from **/etc/multipath.conf** as well.

If you need to use **"1 queue\_if\_no\_path"** and experience the issue noted here, use **dmsetup** to edit the policy at runtime for a particular LUN (i.e. for which all the paths are unavailable).

To illustrate: run **dmsetup message [device] 0 "fail\_if\_no\_path"**, where **[device]** is the multipath device name (e.g. **mpath2**; do not specify the path) for which you want to change the policy from **"queue\_if\_no\_path"** to **"fail\_if\_no\_path"**. ([BZ#419581](#))<sup>24</sup>

- When a LUN is deleted on a configured storage system, the change is not reflected on the host. In such cases, **lvm** commands will hang indefinitely when **dm-multipath** is used, as the LUN has now become *stale*.

To work around this, delete all device and **mpath** link entries in **/etc/lvm/.cache** specific to the stale LUN.

To find out what these entries are, run the following command:

```
ls -l /dev/mpath | grep [stale LUN]
```

For example, if **[stale LUN]** is **3600d0230003414f30000203a7bc41a00**, the following results may appear:

```
lrwxrwxrwx 1 root root 7 Aug  2 10:33 -/3600d0230003414f30000203a7bc41a00 --> ../dm-4
lrwxrwxrwx 1 root root 7 Aug  2 10:33 -/3600d0230003414f30000203a7bc41a00p1 --> ../dm-5
```

This means that **3600d0230003414f30000203a7bc41a00** is mapped to two **mpath** links: **dm-4** and **dm-5**.

As such, the following lines should be deleted from **/etc/lvm/.cache**:

```
/dev/dm-4
/dev/dm-5
/dev/mapper/3600d0230003414f30000203a7bc41a00
```

```
/dev/mapper/3600d0230003414f30000203a7bc41a00p1  
/dev/mpath/3600d0230003414f30000203a7bc41a00  
/dev/mpath/3600d0230003414f30000203a7bc41a00p1
```

[\(BZ#238421\)](#)<sup>26</sup>

- Running the **multipath** command with the **-ll** option can cause the command to hang if one of the paths is on a blocking device. Note that the driver does not fail a request after some time if the device does not respond.

This is caused by the cleanup code, which waits until the path checker request either completes or fails. To display the current **multipath** state without hanging the command, use **multipath -l** instead. [\(BZ#214838\)](#)<sup>27</sup>

## 5.6. dmraid

The dmraid packages contain the ATARAID/DDF1 activation tool that supports RAID device discovery, RAID set activation, and displays properties for ATARAID/DDF1 formatted RAID sets on Linux kernels using device-mapper.

- The **/etc/cron.d/dmeventd-logwatch** crontab file does not specify the user that the logwatch process should be executed by. To work around this issue, the functional portion of this crontab must be changed to:

```
* * * * * root -/usr/sbin/logwatch ---service dmeventd ---range today ---detail med
```

[\(BZ#516892\)](#)<sup>28</sup>

- The installation procedure stores the name of RAID volume and partition in an initscript. When the system boots, dmraid enables the RAID partition (that are named implicitly in the init script. This action functions until the volume and partition names are changed. In these cases, the system may not boot, and the user is given an option to reboot system and start the rebuild procedure in OROM.

OROM changes the name of RAID volume (as seen by dmraid) and dmraid cannot recognize the array identified by previous name stored in initscript. The system no longer boots from RAID partition, since it is not enabled by dmraid. In case of RAID 1 (mirror), the system may be booted from disk that is part of RAID volume. However, dmraid does not allow to active or rebuild the volume which component in mounted.

To work around this issue, do not rebuild the RAID array in OROM. Start the rebuild procedure by dmraid in the operating system, which performs all the steps of rebuilding. dmraid does not change the RAID volume name, therefore the system can be booted from RAID array without the need of init script modification.

To modify init script after OROM has started rebuild:

1. Start the system in rescue mode from the installation disk, skip finding and mounting previous installations.
2. At the command line, find and enable the raid volume that is to be booted from (the RAID volume and partitions will be activated)

```
dmraid --ay isw_effjffhbi_Volume0
```

## 3. Mount the root partition:

```
mkdir -/tmp/raid
mount -/dev/mapper/isw_effjffhbi_Volume0p1 -/tmp/raid
```

## 4. Decompress the boot image:

```
mkdir -/tmp/raid/tmp/image
cd -/tmp/raid/tmp/image
gzip --cd -/tmp/raid/boot/inird-2.6.18-155.el5.img -| cpio --imd --quiet
```

## 5. Change the names of the RAID volumes in the initscript to use the new names of RAID:

```
dmraid --ay --I --p --rm_partition -"/dev/mapper/isw_effjffhbi_Volume0"
kpartx --a --p p -"/dev/mapper/isw_effjffhbi_Volume0"
mkrtotdev --t ext3 --o defaults,ro -/dev/mapper/isw_effjffhbi_Volume0p1
```

## 6. compress and copy initrd image with the modified init script to the boot directory

```
cd -/tmp/raid/tmp/image
find . --print -| cpio --c --o -| gzip --9 > -/tmp/raid/boot/inird-2.6.18-155.el5.img
```

## 7. unmount the raid volume and reboot the system:

```
umount -/dev/mapper/isw_effjffhbi_Volume0p1
dmraid --an
```

## 5.7. dogtail

dogtail is a GUI test tool and automation framework that uses assistive technologies to communicate with desktop applications.

- Attempting to run **sniff** may result in an error. This is because some required packages are not installed with **dogtail**. ([BZ#435702](#))<sup>29</sup>

To prevent this from occurring, install the following packages manually:

- libsvg2
- ghostscript-fonts
- pygtk2-libglade

## 5.8. firstboot

The firstboot utility runs after installation. It guides the user through a series of steps that allows for easier configuration of the machine.

The following notes apply to s390x Architectures:

- The *IBM System z* does not provide a traditional Unix-style physical console. As such, Red Hat Enterprise Linux 5.2 for the *IBM System z* does not support the *firstboot* functionality during initial program load.

To properly initialize setup for Red Hat Enterprise Linux 5.2 on the *IBM System z*, run the following commands after installation:

- `/usr/bin/setup` — provided by the `setuptools` package.
- `/usr/bin/rhn_register` — provided by the `rhn-setup` package.

[\(BZ#217921\)](#)<sup>30</sup>

### 5.9. gfs2-utils

The `gfs2-utils` packages provide the user-level tools necessary to mount, create, maintain and test GFS2 file systems.

If `gfs2` is used as the root file system, the first boot attempt will fail with the error message "**fsck.gfs2: invalid option -- a**". To work around this issue:

1. Enter the root password when prompted
2. Mount the root file system manually:

```
mount --o remount,rw -/dev/VolGroup00/LogVol100 -/
```

3. Edit the `/etc/fstab` file from:

```
/dev/VolGroup00/LogVol100 -/ gfs2 defaults 1 1
```

to

```
/dev/VolGroup00/LogVol100 -/ gfs2 defaults 1 0
```

4. Reboot the system.



#### Important

Note, however that using GFS2 as the root filesystem is unsupported.

### 5.10. gnome-volume-manager

The GNOME Volume Manager monitors volume-related events and responds with user-specified policy. The GNOME Volume Manager can automount hot-plugged drives, automount inserted removable media, autorun programs, automatically play audio CDs and video DVDs, and automatically import photos from a digital camera.

- Removable storage devices (such as CDs and DVDs) do not automatically mount when you are logged in as root. As such, you will need to manually mount the device through the graphical file manager. ([BZ#209362](#))<sup>31</sup>

Alternatively, you can run the following command to mount a device to **/media**:

```
mount -/dev/[device name] -/media
```

## 5.11. initscripts

The initscripts package contains system scripts to boot your system, change runlevels, activate and deactivate most network interfaces, and shut the system down cleanly.

- On systems with more than two encrypted block devices, anaconda has a option to provide a global passphrase. The init scripts, however, do not support this feature. When booting the system, entering each individual passphrase for all encrypted devices will be required. ([BZ#464895](#))<sup>32</sup>
- Boot-time logging to **/var/log/boot.log** is not available in Red Hat Enterprise Linux 5.3. ([BZ#223446](#))<sup>35</sup>, ([BZ#210136](#))<sup>36</sup>

## 5.12. iscsi-initiator-utils

The iscsi package provides the server daemon for the iSCSI protocol, as well as the utility programs used to manage it. iSCSI is a protocol for distributed disk access using SCSI commands sent over Internet Protocol networks.

- iSCSI iface binding is not supported during install or boot. The initiator only supports the ability to log into target portals using the default behavior where the initiator uses the network routing table to decide which NIC to use.

To work around this limitation, booting or installation can be done using the default behavior. After the iscsi and iscsid services start, the iscsi service can log into the target using iSCSI iface binding. This however, will leave an extra session using the default behavior, and it has to be manually logged out using the following command:

```
iscsiadm --m node --T target --p ip --I default --u
```

([BZ#500273](#))<sup>37</sup>

## 5.13. kernel-xen

- Migrating a guest that is using the xen-vnif drivers as a fully virtualized guest under Xen will produce a deadlock in the XenBus. This bug, however, does not present if the IOEMU driver is used or if the system has no active network interface. ([BZ#555910](#))<sup>38</sup>
- On Intel platforms with VT-d enabled, the frame buffer of a fully-virtualized Xen guest with 4GB or more RAM might not be displayed correctly. To work around this issue, create the guest with additional memory (e.g. 2GB more than desired), close the guest, then recreate the guest with the desired amount of RAM. ([BZ#511398](#))<sup>39</sup>



- Xen guests will not boot using configurations that bind multiple virtualized CPUs to a single CPU. ([BZ#570056](#)<sup>40</sup>)
- The Xen hypervisor will not start when booting from an iSCSI disk. To work around this issue, disable the Xen hypervisor's EDD feature with the "edd=off" kernel parameter. For example:

```
kernel -/xen.gz edd=off
```

([BZ#568336](#)<sup>41</sup>)

- Some BIOS implementations initialize interrupt remapping hardware in a way that Xen does not expect. Consequently, a system might hang during boot, returning the error message:

```
(XEN) [VT-D]intremap.c:73: remap_entry_to_ioapic_rte: index (74) is larger than remap  
table entry size (55)!
```

To work around this issue, disable the interrupt remapping feature in the BIOS and reboot the system. ([BZ#563546](#)<sup>42</sup>)

- blkatap may not function as expected, resulting in slow disk I/O causing the guest to operate slowly also. To work around this issue guests should be installed using a physical disk (i.e. a real partition or a logical volume). ([BZ#545692](#)<sup>43</sup>)
- On certain platforms, the mptsas driver may cause kernel warning messages such as the following to be displayed:

```
kernel unaligned access to 0xe0000034f327f0ff, ip=0xa0000002040c4870  
kernel unaligned access to 0xe0000034f327cbff, ip=0xa0000002040c4870  
kernel unaligned access to 0xe00000300c9581ff, ip=0xa0000002040c4870
```

These messages do not indicate a serious error. The data alignment issue will be fixed in a future release. [BZ#570000](#)<sup>44</sup>

- When booting paravirtualized guests that support gigabyte page tables (i.e. a Fedora 11 guest) on Red Hat Enterprise Linux 5.4 Xen, the domain may fail to start if more than 2047MB of memory is configured for the domain. To work around this issue, pass the "**nogbpages**" parameter on the guest kernel command-line. ([BZ#502826](#))<sup>45</sup>
- Boot parameters are required to enable SR/IOV Virtual Function devices. SR/IOV Virtual Function devices can only be accessed if the parameter `pci_pt_e820_access=on` is added to the boot stanza in the `/boot/grub/grub.conf` file. For example:

```
title Red Hat Enterprise Linux Server (2.6.18-152.el5xen)  
    root (hd0,1)  
    kernel -/xen.gz-2.6.18-152.el5 com1=115200,8n1 console=com1 iommu=1  
    module -/vmlinuz-2.6.18-152.el5xen ro root=LABEL=/ console=ttyS0,115200  
pci_pt_e820_access=on
```

This enables the MMCONF access method for the PCI configuration space, a requirement for VF device support

- When using Single Root I/O Virtualization (SR-IOV) devices under Xen, a single Hardware Virtual Machine (HVM) guest is limited to 12 Virtual Function (VF) assignments. [\(BZ#511403\)](#)<sup>46</sup>
- When booting a fully virtualized Xen guest, the following message may be displayed on the guest console:

```
testing NMI watchdog -... <4>
WARNING: CPU#0: NMI appears to be stuck (0->0)!
```

This issue is caused by an implementation issue with the Xen hypervisor and can be safely ignored. [\(BZ#500845\)](#)<sup>47</sup>

- Diskette drive media will not be accessible when using the virtualized kernel. To work around this, use a USB-attached diskette drive instead.

Note that diskette drive media works well with other non-virtualized kernels. [\(BZ#401081\)](#)<sup>48</sup>

- Formatting a disk when running **Windows 2008** or **Windows Vista** as a guest can crash when the guest has been booted with multiple virtual CPUs. To work around this, boot the guest with a single virtual CPU when formatting. [\(BZ#441627\)](#)<sup>49</sup>
- Fully virtualized guests cannot correct for time lost due to the domain being paused and unpaused. Being able to correctly track the time across pause and unpauses is one of the advantages of paravirtualized kernels. This issue is being addressed upstream with replaceable timers, so fully virtualized guests will have paravirtualized timers. Currently, this code is under development upstream and should be available in later versions of Red Hat Enterprise Linux. [\(BZ#422531\)](#)<sup>50</sup>

The following note applies to x86\_64 Architectures:

- Upgrading a host (**dom0**) system to Red Hat Enterprise Linux 5.2 may render existing Red Hat Enterprise Linux 4.5 SMP paravirtualized guests unbootable. This is more likely to occur when the host system has more than 4GB of RAM.

To work around this, boot each Red Hat Enterprise Linux 4.5 guest in single CPU mode and upgrade its kernel to the latest version (for Red Hat Enterprise Linux 4.5.z). [\(BZ#253087\)](#)<sup>51</sup>, [\(BZ#251013\)](#)<sup>52</sup>

The following note applies to the ia64 Architecture:

- On some *Itanium* systems configured for console output to VGA, the **dom0** virtualized kernel may fail to boot. This is because the virtualized kernel failed to properly detect the default console device from the *Extensible Firmware Interface* (EFI) settings.

When this occurs, add the boot parameter **console=tty** to the kernel boot options in **/boot/efi/eliilo.conf**. [\(BZ#249076\)](#)<sup>53</sup>

- On some *Itanium* systems (such as the *Hitachi Cold Fusion 3e*), the serial port cannot be detected in **dom0** when VGA is enabled by the EFI Maintenance Manager. As such, you need to supply the following serial port information to the **dom0** kernel:
  - Speed in bits/second
  - Number of data bits

- Parity
- `io_base` address

These details must be specified in the `append=` line of the `dom0` kernel in `/boot/efi/elilo.conf`. For example:

```
append="com1=19200,8n1,0x3f8 -- quiet rhgb console=tty0  
console=ttyS0,19200n8"
```

In this example, `com1` is the serial port, `19200` is the speed (in bits/second), `8n1` specifies the number of data bits/parity settings, and `0x3f8` is the `io_base` address. ([BZ#433771](#))<sup>54</sup>

- Virtualization does not work on some architectures that use Non-Uniform Memory Access (NUMA). As such, installing the virtualized kernel on systems that use NUMA will result in a boot failure.

Some installation numbers install the virtualized kernel by default. If you have such an installation number and your system uses NUMA and does not work with kernel-xen, deselect the Virtualization option during installation. ([BZ#293071](#))<sup>55</sup>

## 5.14. kernel

### The Kernel

- Attempting to boot the x86 kernel on AMD Magny-Cours systems may result in a kernel panic. A fix will be made available in Red Hat Enterprise Linux 5.5 z-stream updates. To work around this issue, install the x86 variant of Red Hat Enterprise Linux 5.4 and upgrade to Red Hat Enterprise Linux 5.5.z. ([BZ#575799](#))<sup>56</sup>
- A kernel panic may be triggered by the `lpfc` driver when multiple Emulex OneConnect Universal Converged Network Adapter initiators are included in the same Storage Area Network (SAN) zone. Typically, this kernel panic will present after a cable is pulled or one of the systems is rebooted. To work around this issue, configure the SAN to use single initiator zoning. ([BZ#574858](#))<sup>57</sup>
- Systems containing AMD64 or Intel64 based hardware that use the x86 PAE kernel variant may fail to perform a core dump. AMD64 or Intel64 based hardware is able to handle more than 64GB of RAM, but the PAE kernel is strictly limited to 64GB. `kexec-tools` is aware of memory over the 64GB limit, but is unable to access it or produce a `vmcore` file. ([BZ#559928](#))<sup>58</sup>
- Hot-adding memory is not a supported action in Red Hat Enterprise Linux 5.5. However, with Nehalem-EX processors, hot-adding memory must be performed at the same time as hot-adding a CPU. Consequently, hot-adding a CPU is also not a supported action on Nehalem-EX processors. ([BZ#515298](#))
- If a Huawei USB modem is unplugged from a system, the device may not be detected when it is attached again. To work around this issue, the `usbserial` and `usb-storage` driver modules need to be reloaded, allowing the system to detect the device. Alternatively, the if the system is rebooted, the modem will be detected also. ([BZ#517454](#))<sup>59</sup>
- Memory on-line is not currently supported with the Boxboro-EX platform. ([BZ#515299](#))<sup>60</sup>
- Unloading a PF (SR-IOV Physical function) driver from a host when a guest is using a VF (virtual function) from that device can cause a host crash. A PF driver for an SR-IOV device should not be

unloaded until after all guest virtual machines with assigned VFs from that SR-IOV device have terminated. ([BZ#514360](#)<sup>61</sup>)

- Under some circumstances, the sky2 driver may hang, returning the following error message:

```
sky2 eth<N>: receiver hang detected
```

Currently, the only work around to make the device online again is to reboot the system. This bug will be repaired in an upcoming update to Red Hat Enterprise Linux 5.4. ([BZ#509891](#)<sup>62</sup>, [BZ#517976](#))<sup>63</sup>

- Data corruption on NFS filesystems might be encountered on network adapters without support for error-correcting code (ECC) memory that also have TCP segmentation offloading (TSO) enabled in the driver. Note: data that might be corrupted by the sender still passes the checksum performed by the IP stack of the receiving machine A possible work around to this issue is to disable TSO on network adapters that do not support ECC memory. [BZ#504811](#)<sup>64</sup>
- After installation, a System z machine with a large number of memory and CPUs (e.g. 16 CPU's and 200GB of memory) might may fail to IPL. To work around this issue, change the line

```
ramdisk=/boot/initrd-2.6.18-<kernel-version-number>.el5.img
```

to

```
ramdisk=/boot/initrd-2.6.18-<kernel-version-number>.el5.img,0x02000000
```

The command **zipl -V** should now show **0x02000000** as the starting address for the initial RAM disk (initrd). Stop the logical partiton (LPAR), and then manually increase the the storage size of the LPAR.

- On certain hardware configurations the kernel may panic when the Broadcom iSCSI offload driver (**bnx2i.ko** and **cnic.ko**) is loaded. To work around this do not manually load the bnx2i or cnic modules, and temporarily disable the **iscsi** service from starting. To disable the iscsi service, run

```
chkconfig ---del iscsi
chkconfig ---del iscsid
```

On the first boot of your system, the **iscsi** service may start automatically. To bypass this, during bootup, enter interactive start up and stop the iscsi service from starting.

- In Red Hat Enterprise Linux 5, invoking the kernel system call "setpriority()" with a "which" parameter of type "PRIO\_PROCESS" does not set the priority of child threads. ([BZ#472251](#))<sup>65</sup>
- Physical CPUs cannot be safely placed offline or online when the 'kvm\_intel' or 'kvm\_amd' module is loaded. This precludes physical CPU offline and online operations when KVM guests that utilize processor virtualization support are running. It also precludes physical CPU offline and online operations without KVM guests running when the 'kvm\_intel' or 'kvm\_amd' module is simply loaded and not being used.

If the `kmod-kvm` package is installed, the `'kvm_intel'` or `'kvm_amd'` module automatically loads during boot on some systems. If a physical CPU is placed offline while the `'kvm_intel'` or `'kvm_amd'` module is loaded a subsequent attempt to online that CPU may fail with an I/O error.

To work around this issue, unload the `'kvm_intel'` or `'kvm_amd'` before performing physical CPU hot-plug operations. It may be necessary to shut down KVM guests before the `'kvm_intel'` or `'kvm_amd'` will successfully unload.

For example, to offline a physical CPU 6 on an Intel based system:

```
# rmmod kvm_intel
# echo 0 > /sys/devices/system/cpu/cpu6/online
# modprobe kvm_intel
```

[\(BZ#515557\)](#)<sup>66</sup>

- A change to the `cciss` driver in Red Hat Enterprise Linux 5.4 made it incompatible with the `"echo disk > /sys/power/state"` suspend-to-disk operation. Consequently, the system will not suspend properly, returning messages such as:

```
Stopping tasks:
=====
stopping tasks timed out after 20 seconds (1 tasks remaining):
  cciss_scan00
Restarting tasks...<6> Strange, cciss_scan00 not stopped
done
```

[\(BZ#513472\)](#)<sup>67</sup>

- The kernel is unable to properly detect whether there is media present in a CD-ROM drive during kickstart installs. The function to check the presence of media incorrectly interprets the "logical unit is becoming ready" sense, returning that the drive is ready when it is not. To work around this issue, wait several seconds between inserting a CD and asking the installer (`anaconda`) to refresh the CD. [\(BZ#510632\)](#)<sup>68</sup>
- When a `cciss` device is under high I/O load, the `kdump` kernel may panic and the `vmcore` dump may not be saved successfully. [\(BZ#509790\)](#)<sup>69</sup>
- Applications attempting to `malloc` memory approximately larger than the size of the physical memory on the node on a NUMA system may hang or appear to stall. This issue may occur on a NUMA system where the remote memory distance, as defined in SLIT, is greater than 20 and RAM based filesystem like `tmpfs` or `ramfs` is mounted.

To work around this issue, unmount all RAM based filesystems (i.e. `tmpfs` or `ramfs`). If unmounting the RAM based filesystems is not possible, modify the application to allocate lesser memory. Finally, if modifying the application is not possible, disable NUMA memory reclaim by running:

```
sysctl vm.zone_reclaim_mode=0
```



## Important

Turning NUMA reclaim negatively effects the overall throughput of the system.

[\(BZ#507360\)](#)<sup>70</sup>

- Configuring IRQ SMP affinity has no effect on some devices that use message signalled interrupts (MSI) with no MSI per-vector masking capability. Examples of such devices include *Broadcom NetXtreme* Ethernet devices that use the **bnx2** driver.

If you need to configure IRQ affinity for such a device, disable MSI by creating a file in **/etc/modprobe.d/** containing the following line:

```
options bnx2 disable_msi=1
```

Alternatively, you can disable MSI completely using the kernel boot parameter **pci=noms**.

[\(BZ#432451\)](#)<sup>71</sup>

- The **smartctl** tool cannot properly read SMART parameters from SATA devices. [\(BZ#429606\)](#)<sup>72</sup>
- *IBM T60* laptops will power off completely when suspended and plugged into a docking station. To avoid this, boot the system with the argument **acpi\_sleep=s3\_bios**. [\(BZ#439006\)](#)<sup>73</sup>
- The *QLogic iSCSI Expansion Card* for the *IBM Bladecenter* provides both ethernet and iSCSI functions. Some parts on the card are shared by both functions. However, the current **qla3xxx** and **qla4xxx** drivers support ethernet and iSCSI functions individually. Both drivers do not support the use of ethernet and iSCSI functions simultaneously.

Because of this limitation, successive resets (via consecutive **ifdown/ifup** commands) may hang the device. To avoid this, allow a 10-second interval after an **ifup** before issuing an **ifdown**. Also, allow the same 10-second interval after an **ifdown** before issuing an **ifup**. This interval allows ample time to stabilize and re-initialize all functions when an **ifup** is issued. [\(BZ#276891\)](#)<sup>74</sup>

- Laptops equipped with the *Cisco Aironet MPI-350* wireless may hang trying to get a DHCP address during any network-based installation using the wired ethernet port.

To work around this, use local media for your installation. Alternatively, you can disable the wireless card in the laptop BIOS prior to installation (you can re-enable the wireless card after completing the installation). [\(BZ#213262\)](#)<sup>75</sup>

- Hardware testing for the *Mellanox MT25204* has revealed that an internal error occurs under certain high-load conditions. When the **ib\_mthca** driver reports a catastrophic error on this hardware, it is usually related to an insufficient completion queue depth relative to the number of outstanding work requests generated by the user application.

Although the driver will reset the hardware and recover from such an event, all existing connections at the time of the error will be lost. This generally results in a segmentation fault in the user application. Further, if **opensm** is running at the time the error occurs, then you need to manually restart it in order to resume proper operation. [\(BZ#251934\)](#)<sup>76</sup>

- If your system uses the TSC timer, the **gettimeofday** system call may move backwards. This is because of an overflow issue that causes the TSC timer to jump forward significantly in some cases; when this occurs, the TSC timer will correct itself, but will ultimately register a movement backwards in time.

This issue is particularly critical for time-sensitive systems, such as those used for transaction systems and databases. As such, if your system needs precision timing, Red Hat strongly recommends that you set the kernel to use another timer (for example, HPET). ([BZ#443435](#))<sup>77</sup>

- The *IBM T41* laptop model does not enter **Suspend Mode** properly; as such, **Suspend Mode** will still consume battery life as normal. This is because Red Hat Enterprise Linux 5 does not yet include the **radeonfb** module.

To work around this, add a script named **hal-system-power-suspend** to **/usr/share/hal/scripts/** containing the following lines:

```
chvt 1
radeontool light off
radeontool dac off
```

This script will ensure that the *IBM T41* laptop enters **Suspend Mode** properly. To ensure that the system resumes normal operations properly, add the script **restore-after-standby** to the same directory as well, containing the following lines:

```
radeontool dac on
radeontool light on
chvt 7
```

([BZ#227496](#))<sup>78</sup>

- If the **edac** module is loaded, BIOS memory reporting will not work. This is because the **edac** module clears the register that the BIOS uses for reporting memory errors.

The current Red Hat Enterprise Linux Driver Update Model instructs the kernel to load all available modules (including the **edac** module) by default. If you wish to ensure BIOS memory reporting on your system, you need to manually blacklist the **edac** modules. To do so, add the following lines to **/etc/modprobe.conf**:

```
blacklist edac_mc
blacklist i5000_edac
blacklist i3000_edac
blacklist e752x_edac
```

([BZ#441329](#))<sup>79</sup>

- Due to outstanding driver issues with hardware encryption acceleration, users of Intel WiFi Link 4965, 5100, 5150, 5300, and 5350 wireless cards are advised to disable hardware accelerated encryption using module parameters. Failure to do so may result in the inability to connect to Wired Equivalent Privacy (WEP) protected wireless networks after connecting to WiFi Protected Access (WPA) protected wireless networks.



To do so, add the following options to `/etc/modprobe.conf`:

```
alias wlan0 iwlagn
options iwlagn swcrypto50=1 swcrypto=1
```

(where `wlan0` is the default interface name of the first Intel WiFi Link device)

[\(BZ#468967\)](#)<sup>81</sup>

The following note applies to PowerPC Architectures:

- The size of the PPC kernel image is too large for OpenFirmware to support. Consequently, network booting will fail, resulting in the following error message:

```
Please wait, loading kernel...
/pci@8000000f8000000/ide@4,1/disk@0:2,vmlinux-anaconda: No such file or directory
boot:
```

To work around this:

1. Boot to the OpenFirmware prompt, by pressing the '8' key when the IBM splash screen is displayed.
2. Run the following command:

```
setenv real-base 2000000
```

3. Boot into System Management Services (SMS) with the command:

```
0> dev -/packages/gui obe
```

[\(BZ#462663\)](#)<sup>82</sup>

## 5.15. kexec-tools

kexec-tools provides the `/sbin/kexec` binary that facilitates a new kernel to boot using the kernel's kexec feature either on a normal or a panic reboot. This package contains the `/sbin/kexec` binary and ancillary utilities that together form the userspace component of the kernel's kexec feature

- Executing `kdump` on an *IBM Bladecenter QS21* or *QS22* configured with NFS root will fail. To avoid this, specify an NFS dump target in `/etc/kdump.conf`. [\(BZ#368981\)](#)<sup>83</sup>
- Some `forcedeth` based devices may encounter difficulty accessing memory above 4GB during operation in a `kdump` kernel. To work around this issue, add the following line to the `/etc/sysconfig/kdump` file:

```
KDUMP_COMMANDLINE_APPEND="dma_64bit=0"
```

This work around prevents the forcedeth network driver from using high memory resources in the `kdump` kernel, allowing the network to function properly.

- The system may not successfully reboot into a **kexec/kdump** kernel if X is running and using a driver other than `vesa`. This problem only exists with *ATI Rage XL* graphics chipsets.

If X is running on a system equipped with *ATI Rage XL*, ensure that it is using the `vesa` driver in order to successfully reboot into a **kexec/kdump** kernel. [\(BZ#221656\)](#)<sup>84</sup>

- **kdump** now serializes drive creation registration with the rest of the **kdump** process. Consequently, **kdump** may hang waiting for IDE drives to be initialized. In these cases, it is recommended that IDE disks not be used with **kdump**. [\(BZ#473852\)](#)<sup>86</sup>
- It is possible in rare circumstances, for **makedumpfile** to produce erroneous results but not have them reported. This is due to the fact that **makedumpfile** processes its output data through a pipeline consisting of several stages. If **makedumpfile** fails, the other stages will still succeed, effectively masking the failure. Should a `vmcore` appear corrupt, and **makedumpfile** is in use, it is recommended that the core be recorded without **makedumpfile** and a bug be reported. [\(BZ#475487\)](#)<sup>87</sup>
- **kdump** now restarts when CPUs or DIMMs are hot-added to a system. If multiple items are added at the same time, several sequential restarts may be encountered. This behavior is intentional, as it minimizes the time-frame where a crash may occur while memory or processors are not being tracked by **kdump**. [\(BZ#474409\)](#)<sup>88</sup>

The following note applies to ia64 Architecture:

- Some *Itanium* systems cannot properly produce console output from the **kexec purgatory** code. This code contains instructions for backing up the first 640k of memory after a crash.

While **purgatory** console output can be useful in diagnosing problems, it is not needed for **kdump** to properly function. As such, if your *Itanium* system resets during a **kdump** operation, disable console output in **purgatory** by adding `--noio` to the `KEXEC_ARGS` variable in `/etc/sysconfig/kdump`. [\(BZ#436426\)](#)<sup>89</sup>

### 5.16. krb5

Kerberos 5 is a network authentication system which authenticates clients and servers to each other using symmetric key encryption and a trusted third party, the KDC.

- The format of a stash file, while not architecture-specific, is endian-specific. Consequently, a stash file is not directly portable between big-endian and little-endian systems. When setting up a secondary KDC where the endianness differs from that of the master KDC, the stash file should be recreated by running `'kdb5_util create -s'` on the secondary and supplying the original master password. [\(BZ#514741\)](#)<sup>90</sup>

### 5.17. kvm

Kernel-based Virtual Machine (KVM) is a full virtualization solution for Linux on x86 hardware.

KVM is a Linux kernel module built for the standard Red Hat Enterprise Linux kernel. KVM can run multiple unmodified, virtualized guest Windows and Linux operating systems. KVM is a hypervisor which uses the `libvirt` virtualization tools (`virt-manager` and `virsh`).

- By default, KVM virtual machines created in Red Hat Enterprise Linux 5.5 have a virtual Realtek 8139 (rtl8139) network interface controller (NIC). The rtl8139 virtual NIC works fine in most environments, but may suffer from performance degradation issues on some networks for example, a 10 GigE (10 Gigabit Ethernet) network.

One workaround for this issue is switch to a different type of virtual NIC, for example, Intel PRO/1000 (e1000) or virtio (a virtual I/O driver for Linux that can talk to the hypervisor).

To switch to e1000:

1. Shutdown the guest OS
2. Edit the guest OS definition with the command-line tool virsh:

```
virsh edit GUEST
```

3. Locate the network interface section and add a model line as shown:

```
<interface type='network'>
...
<model type='e1000' -/>
</interface>
```

4. Save the changes and exit the text editor
5. Restart the guest OS

Alternatively, if you're having trouble installing the OS on the virtual machine because of the rtl8139 NIC (for example, because you're installing the OS over the network), you can create a virtual machine from scratch with an e1000 NIC. This method requires you to have at least one virtual machine already created (possibly installed from CD or DVD) to use as a template.

1. Create an XML template from an existing virtual machine:

```
virsh dumpxml GUEST > ~/tmp/guest.xml
```

2. Copy and edit the XML file and update the unique fields: virtual machine name, UUID, disk image, MAC address, etc. NOTE: you can delete the UUID and MAC address lines and virsh will generate a UUID and MAC address.

```
cp ~/tmp/guest.xml ~/tmp/new-guest.xml
vi ~/tmp/new-guest.xml
```

3. Locate the network interface section and add a model line as shown:

```
<interface type='network'>
...
<model type='e1000' -/>
</interface>
```

4. Create the new virtual machine:

```
virsh define -/tmp/new-guest.xml
virsh start new-guest
```

- Currently, KVM cannot disable virtualization extensions on a CPU while it is being taken down. Consequently, suspending a host running KVM-based virtual machines may cause the host to crash. ([BZ#509809](#))<sup>91</sup>
- The KSM module shipped in this release is a different version from the KSM module found on the latest upstream kernel versions. Newer features, such as exporting statistics on the /sys filesystem, that are implemented upstream are not in the version shipped in this release.
- The mute button in the audio control panel on a Windows virtual machine does not mute the sound. [BZ#482570](#)<sup>92</sup>
- Hot-unplugging of PCI devices is not supported in this release. This feature will be introduced in a future update. ([BZ#510679](#))<sup>93</sup>
- When migrating KVM guests between hosts, the NX CPU feature setting on both source and destination must match. Migrating a guest between a host with the NX feature disabled (i.e. disabled in the BIOS settings) and a host with the NX feature enabled may cause the guest to crash. ([BZ#516029](#))<sup>94</sup>
- the application binary interface (ABI) between the KVM userspace (e.g. qemu-kvm) and the KVM kernel modules may change in future updates. Using the latest upstream qemu-kvm package is unsupported due to ABI differences. ([BZ#515549](#))<sup>95</sup>
- Devices using the qlge driver cannot be assigned to a KVM guest using KVM's PCI Device Driver assignment. ([BZ#507689](#))<sup>96</sup>
- the use of the qcow2 disk image format with KVM is considered a Technology Preview. ([BZ#517880](#))<sup>97</sup>
- 64-bit versions of Windows 7 do not have support for the AC'97 Audio Codec. Consequently, the virtualized sound device Windows 7 kvm guests will not function. ([BZ#563122](#))<sup>98</sup>
- Hotplugging emulated devices after migration may result in the virtual machine crashing after a reboot or the devices no longer being visible. ([BZ#507191](#))<sup>99</sup>
- Windows 2003 32-bit guests with more than 4GB of RAM may crash on reboot with the default qemu-kvm CPU settings. To work around this issue, configure a different CPU model on the management interface. ([BZ#516762](#))<sup>100</sup>
- The KVM modules from the **kmod-kvm** package do not support kernels prior to version 2.6.18-159.el5. Error messages similar to the following will be returned if attempting to install these modules on older kernels:

```
FATAL: Error inserting kvm_intel
(/lib/modules/2.6.18-155.el5/weak-updates/kmod-kvm/kvm-intel.ko): Unknown
symbol in module, or unknown parameter (see dmesg)
```

([BZ#509361](#))<sup>101</sup>

- the **kvm** package has incorrect dependencies related to the **libgcrypt** package. Consequently, if the **libgcrypt** package installed on a system is earlier than version 1.4.4, the **qemu-kvm** process may refuse to start, returning a **libgcrypt initialization error** message. To work around this issue, update **libgcrypt** to the version provided by Red Hat Enterprise Linux 5.5. ([BZ#503118](#))<sup>102</sup>
- The KVM modules available in the **kmod-kvm** package are loaded automatically at boot time if the **kmod-kvm** package is installed. To make these KVM modules available after installing the **kmod-kvm** package the system either needs to be rebooted or the modules can be loaded manually by running the **/etc/sysconfig/modules/kvm.modules** script. ([BZ#501543](#))<sup>103</sup>
- Some Linux-based guests that use virtio virtual block devices may abort during installation, returning the error message: **unhandled vm exit: 0x31 vcpu\_id 0** To work around this issue, consider utilizing a different interface (other than virtio) for the guest virtual disk. ([BZ#518081](#))<sup>104</sup>
- RHEL5.x virtualization relies on etherboot for remote booting. Etherboot is an implementation of the pxe standard, but lacks some features that are present in the new gppe boot technology which is not shipped with RHEL. It is possible to use the gppe roms with RHEL 5.4. As an example, gppe roms can be used to interpret requests generated by Microsoft RIS or WDS. All components present in RHEL5.4 are capable of booting gppe roms. The roms can be obtained directly from <http://rom-omatic.net/>, or other sources like the Fedora Project. [BZ#509208](#)<sup>105</sup>
- The Preboot eXecution Environment (PXE) boot ROMs included with KVM are from the Etherboot project. Consequently, some bug fixes or features that are present on the newer gPXE project are not available on Etherboot. For example, Virtual Machines (VMs) cannot boot using Microsoft based PXE (ie. Remote Installation Services (RIS) or Windows Deployment Services (WDS)). ([BZ#497692](#))<sup>106</sup>
- The following QEMU / KVM features are currently disabled and not supported: ([BZ#512837](#))<sup>107</sup>
  - smb user directories
  - scsi emulation
  - "isapc" machine type
  - nested KVM guests
  - usb mass storage device emulation
  - usb wacom tablet emulation
  - usb serial emulation
  - usb network emulation
  - usb bluetooth emulation
  - device emulation for vmware drivers
  - sb16, es1370, and ac97 sound card emulation
  - bluetooth emulation

### 5.18. less

The `less` utility is a text file browser that resembles `more`, but with more capabilities ("less is more"). The `less` utility allows users to move backwards in the file as well as forwards. Because `less` need not read the entire input file before it starts, `less` starts up more quickly than text editors (`vi`, for example).

- The "`less`" command has been updated. `less` no longer adds the "carriage return" character when wrapping long lines. Consequently, lines longer than the terminal width will be displayed incorrectly when browsing the file line per line. The command line option "`--old-bot`" forces `less` to behave as it did previously, with long text lines displayed correctly. ([BZ#441691](#))<sup>108</sup>

### 5.19. libcmptutil

`libcmptutil` is a library of utility functions for CMPI providers. Its goal is to reduce the amount of repetitive work done in most CMPI providers by encapsulating common procedures with more "normal" APIs. This includes operations such as retrieving typed instance properties, standardizing method dispatch and argument checking.

- The `libcmptutil-devel` package depends on `tog-pegasus-devel`, which for the Red Hat Enterprise Linux Desktop product is only available from the Workstation option. Therefore, any attempt to install the `libcmptutil-devel` package on a system that does not have a Subscription including the Workstation option or is not subscribed to the Workstation channel on RHN, will fail with an unresolved dependency error.

### 5.20. libvirt

**Problem Description:** The `libvirt` library is a C API for managing and interacting with the virtualization capabilities of Linux and other operating systems. In addition, `libvirt` provides tools for remotely managing virtualized systems.

- Volumes created using the `libvirt` storage API may not have an SELinux label that allows access by virtual machines. If an SELinux AVC denial is reported when starting a Xen or KVM guest, the administrator should either manually relabel the file/device, or add the file path(s) as rule to the SELinux policy using the '`semanage`' tool. ([BZ#510143](#))<sup>109</sup>

### 5.21. lvm2

The `lvm2` package contains support for Logical Volume Management (LVM).

The following are the Known Issues that apply to the `lvm2` packages in Red Hat Enterprise Linux 5.4

- The `lvchange` command is used to change the attributes of a logical volume. Issuing the `lvchange` command on a volume group that contains a mirror or snapshot may result in messages similar to the following:

```
Unable to change mirror log LV fail_secondary_mlog directly
Unable to change mirror image LV fail_secondary_mimage_0 directly
Unable to change mirror image LV fail_secondary_mimage_1 directly
```

These messages can be safely ignored. ([BZ#232499](#))<sup>110</sup>

## 5.22. mesa

Mesa provides a 3D graphics API that is compatible with OpenGL. It also provides hardware-accelerated drivers for many popular graphics chips.

The following note applies to x86\_64 Architectures:

- On an *IBM T61* laptop, Red Hat recommends that you refrain from clicking the **glxgears** window (when **glxgears** is run). Doing so can lock the system.

To prevent this from occurring, disable the tiling feature. To do so, add the following line in the **Device** section of **/etc/X11/xorg.conf**:

```
Option "Tiling" "0"
```

([BZ#444508](#))<sup>111</sup>

## 5.23. mkinitrd

The mkinitrd utility creates file system images for use as initial ramdisk (initrd) images.

- When using an encrypted device, the following error message may be reported during bootup:

```
insmod: error inserting -'/lib/aes_generic.ko': -1 File exists
```

This message can safely be ignored. ([BZ#466296](#))<sup>112</sup>

- Installation using a Multiple Device (MD) RAID on top of multipath will result in a machine that cannot boot. Multipath to Storage Area Network (SAN) devices which provide RAID internally are not affected. ([BZ#467469](#))<sup>113</sup>

The following note applies to s390x Architectures:

- When installing Red Hat Enterprise Linux 5.4, the following errors may be returned in **install.log**:

```
Installing kernel-2.6.18-158.el5.s390x
cp: cannot stat `/sbin/dmraid.static': No such file or directory
```

This message can be safely ignored.

- iSCSI root devices do not function correctly if used over an IPv6 network connection. While the installation will appear to succeed, the system will fail to find the root filesystem during the first boot. ([BZ#529636](#))<sup>114</sup>

## 5.24. openib

The OpenFabrics Alliance Enterprise Distribution (OFED) is a collection of Infiniband and iWARP hardware diagnostic utilities, the Infiniband fabric management daemon, Infiniband/iWARP kernel module loader, and libraries and development packages for writing applications that use Remote Direct Memory Access (RDMA) technology. Red Hat Enterprise Linux uses the OFED software stack as its complete stack for Infiniband/iWARP/RDMA hardware support.



The following note applies to the ia64 Architectures:

- Running **perftest** will fail if different CPU speeds are detected. As such, you should disable CPU speed scaling before running **perftest**. ([BZ#433659](#))<sup>116</sup>

### 5.25. openmpi

Open MPI, MVAPICH, and MVAPICH2 are all competing implementations of the Message Passing Interface (MPI) standard. MVAPICH implements version 1 of the MPI standard, while Open MPI and MVAPICH2 both implement the later, version 2 of the MPI standard.

- **mvapich** and **mvapich2** in Red Hat Enterprise Linux 5 are compiled to support only *InfiniBand/iWARP* interconnects. Consequently, they will not run over ethernet or other network interconnects. ([BZ#466390](#))<sup>117</sup>
- When upgrading **openmpi** using **yum**, the following warning may be returned:

```
cannot open `/tmp/openmpi-upgrade-version.*' for reading: No such file or directory
```

The message is harmless and can be safely ignored. ([BZ#463919](#))<sup>118</sup>

- A bug in previous versions of **openmpi** and **lam** may prevent you from upgrading these packages. This bug manifests in the following error (when attempting to upgrade **openmpi** or **lam**:

```
error: %preun(openmpi-[version]) scriptlet failed, exit status 2
```

As such, you need to manually remove older versions of **openmpi** and **lam** in order to install their latest versions. To do so, use the following **rpm** command:

```
rpm -qa | grep '^openmpi-|^lam-' | xargs rpm -e --noscripts --allmatches  
(BZ#433841)120
```

### 5.26. qspice

The Simple Protocol for Independent Computing Environments (SPICE) is a remote display system built for virtual environments which allows users to view a computing 'desktop' environment not only on the machine where it is running, but from anywhere on the Internet and from a wide variety of machine architectures.

- Occasionally, the video compression algorithm used by SPICE starts when the guest is accessing text instead of video or moving content. This causes the text to appear blurry or difficult to read. ([BZ#493375](#))<sup>121</sup>

### 5.27. systemtap

SystemTap provides an instrumentation infrastructure for systems running the Linux 2.6 kernel. It allows users to write scripts that probe and trace system events for monitoring and profiling purposes. SystemTap's framework allows users to investigate and monitor a wide variety of wide variety of kernel functions, system calls, and other events that occur in both kernel-space and user-space.

The following are the Known Issues that apply to the **systemtap** package in Red Hat Enterprise Linux 5.4

- Running some user-space probe test cases provided by the **systemtap-testsuite** package fail with an **Unknown symbol in module** error on some architectures. These test cases include (but are not limited to):
  - **systemtap.base/uprobes.exp**
  - **systemtap.base/bz10078.exp**
  - **systemtap.base/bz6850.exp**
  - **systemtap.base/bz5274.exp**

Because of a known bug in the latest SystemTap update, new SystemTap installations do not unload old versions of the **uprobes.ko** module. Some updated user-space probe tests provided by the **systemtap-testsuite** package use symbols available only in the latest **uprobes.ko** module (also provided by the latest SystemTap update). As such, running these user-space probe tests result in the error mentioned earlier.

If you encounter this error, simply run **rmmod uprobes** to manually remove the older **uprobes.ko** module before running the user-space probe test again. [\(BZ#499677\)](#)<sup>122</sup>

- SystemTap currently uses GCC to probe user-space events. GCC is, however, unable to provide debuggers with precise location list information for parameters. In some cases, GCC also fails to provide visibility on some parameters. As a consequence, SystemTap scripts that probe user-space may return inaccurate readings. [\(BZ#239065\)](#)<sup>123</sup>

## 5.28. virtio-win

VirtIO para-virtualized Windows(R) drivers for 32-bit and 64-bit Windows (R) guests.

- Low performance with UDP messages larger than 1024 is a known Microsoft issue: <http://support.microsoft.com/default.aspx/kb/235257>. For the message larger than 1024 bytes follow the workaround procedure detailed in the above Microsoft knowledgebase article.

[\(BZ#496592\)](#)<sup>124</sup>

- Installation of Windows XP with the floppy containing guest drivers (in order to get the virtio-net drivers installed as part of the installation), will return messages stating that the viostor.sys file could not be found. viostor.sys is not part of the network drivers, but is on the same floppy as portions of the virtio-blk drivers. These messages can be safely ignored, simply accept the installation's offer to reboot, and the installation will continue normally. [BZ#513160](#)<sup>125</sup>

## 5.29. xorg-x11-drv-i810

xorg-x11-drv-i810 is an Intel integrated graphics video driver for the X.Org implementation of the X Window System.

- Running a screensaver or resuming a suspended laptop with an external monitor attached may result in a blank screen or a brief flash followed by a blank screen. If this occurs with the screensaver, the prompt for your password is being obscured, the password can still be entered blindly to get back to the desktop. To work around this issue, physically disconnect the external monitor and then press the video hotkey (usually Fn-F7) to rescan the available outputs, before suspending the laptop.

The following notes apply to x86\_64 Architectures:

- If your system uses an *Intel 945GM* graphics card, do not use the **i810** driver. You should use the default **intel** driver instead. ([BZ#468218](#))<sup>126</sup>
- On dual-GPU laptops, if one of the graphics chips is Intel-based, the Intel graphics mode cannot drive any external digital connections (including HDMI, DVI, and DisplayPort). This is a hardware limitation of the Intel GPU. If you require external digital connections, configure the system to use the discrete graphics chip (in the BIOS). ([BZ#468259](#))<sup>127</sup>

### 5.30. xorg-x11-drv-nv

xorg-x11-drv-nv provides a driver for NVIDIA cards for the X.org implementation of the X Window System.

- Improvements have been made to the 'nv' driver, enhancing suspend and resume support on some systems equipped with nVidia GeForce 8000 and 9000 series devices. Due to technical limitations, this will not enable suspend/resume on all hardware. ([BZ#414971](#))<sup>128</sup>
- The nv driver for NVIDIA graphics devices does not fully support the DisplayPort digital display interface. Connections from DisplayPort video devices to DisplayPort monitors are unsupported by the nv driver. Internal laptop and notebook displays that use Embedded DisplayPort (eDP) are also unsupported. Other connections, such as VGA, DVI, HDMI and the use of DisplayPort to DVI adapters are supported by the nv driver. To work around this limitation, it is recommended that the "vesa" driver be used. ([BZ#566228](#))<sup>129</sup>

The following note applies to x86\_64 Architectures:

- Some machines that use *NVIDIA* graphics cards may display corrupted graphics or fonts when using the graphical installer or during a graphical login. To work around this, switch to a virtual console and back to the original X host. ([BZ#222737](#))<sup>132</sup>, ([BZ#221789](#))<sup>133</sup>

### 5.31. xorg-x11-drv-vesa

xorg-x11-drv-vesa is a video driver for the X.Org implementation of the X Window System. It is used as a fallback driver for cards with no native driver, or when the native driver does not work.

The following note applies to x86 Architectures:

- When running the bare-metal (non-Virtualized) kernel, the X server may not be able to retrieve **EDID** information from the monitor. When this occurs, the graphics driver will be unable to display resolutions higher than 800x600.

To work around this, add the following line to the **ServerLayout** section of **/etc/X11/xorg.conf**:

```
Option -"Int10Backend" -"x86emu"
```

([BZ#236416](#))<sup>134</sup>

## 5.32. yaboot

The yaboot package is a boot loader for Open Firmware based PowerPC systems. It can be used to boot IBM eServer System p machines.

- If the string that represents the path to kernel (or ramdisk) is greater than 63 characters, network booting an IBM Power5 series system may result in the following error:

```
FINAL File Size = 8948021 bytes.
load-base=0x4000
real-base=0xc00000
DEFAULT CATCH!, exception-handler=fff00300
```

The firmware for IBM Power6 and IBM Power7 systems contains a fix for this issue. ([BZ#550086](#))<sup>135</sup>

## 5.33. xen

- As of Red Hat Enterprise Linux 5.4, PCI devices connected to a single PCI-PCI bridge can no longer be assigned to different PV guests. If the old, unsafe behaviour is required, disable `pci-dev-assign-strict-check` in `/etc/xen/xend-config.sxp`. ([BZ#508310](#))<sup>136</sup>
- In live migrations of paravirtualized guests, time-dependent guest processes may function improperly if the corresponding hosts' (dom0) times are not synchronized. Use NTP to synchronize system times for all corresponding hosts before migration. ([BZ#426861](#))<sup>137</sup>
- When running x86\_64 Xen, it is recommended to set `dom0-min-mem` in `/etc/xen/xend-config.sxp` to a value of 1024 or higher. Lower values may cause the dom0 to run out of memory, resulting in poor performance or out-of-memory situations. ([BZ#519492](#))
- The Red Hat Enterprise Linux 3 kernel does not include SWIOTLB support. SWIOTLB support is required for Red Hat Enterprise Linux 3 guests to support more than 4GB of memory on AMD Opteron and Athlon-64 processors. Consequently, Red Hat Enterprise Linux 3 guests are limited to 4GB of memory on AMD processors. ([BZ#504187](#))<sup>138</sup>
- When setting up interface bonding on **dom0**, the default **network-bridge** script may cause bonded network interfaces to alternately switch between **unavailable** and **available**. This occurrence is commonly known as *flapping*.

To prevent this, replace the standard **network-script** line in `/etc/xen/xend-config.sxp` with the following line:

```
(network-script network-bridge-bonding netdev=bond0)
```

Doing so will disable the *netloop* device, which prevents Address Resolution Protocol (ARP) monitoring from failing during the address transfer process. ([BZ#429154](#))<sup>140</sup>, ([BZ#429154](#))<sup>141</sup>

- The Hypervisor outputs messages regarding attempts by any guest to write to an MSR. Such messages contain the statement **Domain attempted WRMSR**. These messages can be safely ignored; furthermore, they are rate limited and should pose no performance risk. ([BZ#477647](#))<sup>142</sup>

The following note applies to x86\_64 Architectures:

- Installing Red Hat Enterprise Linux 3.9 on a fully virtualized guest may be extremely slow. In addition, booting up the guest after installation may result in **hda: lost interrupt** errors.

To avoid this bootup error, configure the guest to use the SMP kernel. ([BZ#249521](#))<sup>143</sup>

---

# Appendix A. Package Manifest

This appendix is a list of all package changes since the release of Red Hat Enterprise Linux 5.4

## A.1. Added Packages

ctdb-1.0.82-1.el5

- Group: System Environment/Daemons
- Summary: A Clustered Database based on Samba's Trivial Database (TDB)
- Description: CTDB is a cluster implementation of the TDB database used by Samba and other projects to store temporary data. If an application is already using TDB for temporary data it is very easy to convert that application to be cluster aware and use CTDB instead.

freeradius2-2.1.7-7.el5

- Group: System Environment/Daemons
- Summary: High-performance and highly configurable free RADIUS server
- Description: The FreeRADIUS Server Project is a high performance and highly configurable GPL'd free RADIUS server. The server is similar in some respects to Livingston's 2.0 server. While FreeRADIUS started as a variant of the Cistron RADIUS server, they don't share a lot in common any more. It now has many more features than Cistron or Livingston, and is much more configurable. FreeRADIUS is an Internet authentication daemon, which implements the RADIUS protocol, as defined in RFC 2865 (and others). It allows Network Access Servers (NAS boxes) to perform authentication for dial-up users. There are also RADIUS clients available for Web servers, firewalls, Unix logins, and more. Using RADIUS allows authentication and authorization for a network to be centralized, and minimizes the amount of re-configuration which has to be done when adding or deleting new users.

gpxe-0.9.7-8.el5

- Group: System Environment/Base
- Summary: A network boot loader
- Description: gPXE is an open source network bootloader. It provides a direct replacement for proprietary PXE ROMs, with many extra features such as DNS, HTTP, iSCSI, etc.

gsl-1.13-3.el5

- Group: System Environment/Libraries
- Summary: The GNU Scientific Library for numerical analysis
- Description: The GNU Scientific Library (GSL) is a collection of routines for numerical analysis, written in C.

postgresql84-8.4.2-5.el5

- Group: Applications/Databases
- Summary: PostgreSQL client programs

- Description: PostgreSQL is an advanced Object-Relational database management system (DBMS) that supports almost all SQL constructs (including transactions, subselects and user-defined types and functions). The postgresql package includes the client programs and libraries that you'll need to access a PostgreSQL DBMS server. These PostgreSQL client programs are programs that directly manipulate the internal structure of PostgreSQL databases on a PostgreSQL server. These client programs can be located on the same machine with the PostgreSQL server, or may be on a remote machine which accesses a PostgreSQL server over a network connection. This package contains the docs in HTML for the whole package, as well as command-line utilities for managing PostgreSQL databases on a PostgreSQL server. If you want to manipulate a PostgreSQL database on a local or remote PostgreSQL server, you need this package. You also need to install this package if you're installing the postgresql-server package.

### python-dmidecode-3.10.8-4.el5

- Group: System Environment/Libraries
- Summary: Python module to access DMI data
- Description: python-dmidecode is a python extension module that uses the code-base of the 'dmidecode' utility, and presents the data as python data structures or as XML data using libxml2.

### samba3x-3.3.8-0.51.el5

- Group: System Environment/Daemons
- Summary: Server and Client software to interoperate with Windows machines
- Description: Samba is the suite of programs by which a lot of PC-related machines share files, printers, and other information (such as lists of available files and printers). The Windows NT, OS/2, and Linux operating systems support this natively, and add-on packages can enable the same thing for DOS, Windows, VMS, UNIX of all kinds, MVS, and more. This package provides an SMB/CIFS server that can be used to provide network services to SMB/CIFS clients. Samba uses NetBIOS over TCP/IP (NetBT) protocols and does NOT need the NetBEUI (Microsoft Raw NetBIOS frame) protocol.

### tunctl-1.5-3.el5

- Group: Applications/System
- Summary: Create and remove virtual network interfaces
- Description: tunctl is a tool to set up and maintain persistent TUN/TAP network interfaces, enabling user applications access to the wire side of a virtual network interface. Such interfaces is useful for connecting VPN software, virtualization, emulation and a number of other similar applications to the network stack. tunctl originates from the User Mode Linux project.

### xz-4.999.9-0.3.beta.20091007git.el5

- Group: Applications/File
- Summary: LZMA compression utilities
- Description: XZ Utils are an attempt to make LZMA compression easy to use on free (as in freedom) operating systems. This is achieved by providing tools and libraries which are similar to use than the equivalents of the most popular existing compression algorithms. LZMA is a

general purpose compression algorithm designed by Igor Pavlov as part of 7-Zip. It provides high compression ratio while keeping the decompression speed fast.

## A.2. Dropped Packages

libpfm-3.2-0.060926.4.el5

- Group: Development/Libraries
- Summary: a performance monitoring library for Linux/ia64
- Description: This package contains a library to develop performance monitoring applications using the Performance Monitor Unit (PMU) available on various processors.

pfmon-3.2-0.060926.5.el5

- Group: Development/Tools
- Summary: a performance monitoring tool for Linux/ia64
- Description: This package contains pfmon 3.x, a tool to monitor performance using the Performance Monitor Unit (PMU). Pfmom can monitor standalone programs or the entire system on both UP and SMP Linux systems. This version of pfmon requires a kernel perfmon-2.x (found in 2.6 kernels) subsystem to function properly.

## A.3. Updated Packages

NetworkManager-0.7.0-9.el5 - NetworkManager-0.7.0-10.el5

- Group: System Environment/Base
- Summary: Network connection manager and user applications
- Description: NetworkManager attempts to keep an active network connection available at all times. It is intended only for the desktop use-case, and is not intended for usage on servers. The point of NetworkManager is to make networking configuration and setup as painless and automatic as possible. If using DHCP, NetworkManager is intended to replace default routes, obtain IP addresses from a DHCP server, and change nameservers whenever it sees fit.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

OpenIPMI-2.0.16-5.el5 - OpenIPMI-2.0.16-7.el5

- Group: System Environment/Base



## Appendix A. Package Manifest

---

- Summary: OpenIPMI (Intelligent Platform Management Interface) library and tools
- Description: The Open IPMI project aims to develop an open code base to allow access to platform information using Intelligent Platform Management Interface (IPMI). This package contains the tools of the OpenIPMI project.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

### PyXML-0.8.4-4 - PyXML-0.8.4-4.el5\_4.2

- Group: Development/Libraries
- Summary: XML libraries for python.
- Description: An XML package for Python. The distribution contains a validating XML parser, an implementation of the SAX and DOM programming interfaces and an interface to the Expat parser.
- Added Dependencies:
  - expat-devel
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

### acl-2.2.39-3.el5 - acl-2.2.39-6.el5

- Group: System Environment/Base
- Summary: Access control list utilities.
- Description: This package contains the getfacl and setfacl utilities needed for manipulating access control lists.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

acpid-1.0.4-9.el5 - acpid-1.0.4-9.el5\_4.2

- Group: System Environment/Daemons
- Summary: ACPI Event Daemon
- Description: acpid is a daemon that dispatches ACPI events to user-space programs.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

aide-0.13.1-4.el5 - aide-0.13.1-6.el5

- Group: Applications/System
- Summary: Intrusion detection environment
- Description: AIDE (Advanced Intrusion Detection Environment) is a file integrity checker and intrusion detection program.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts

## Appendix A. Package Manifest

---

- No removed conflicts
- No added obsoletes
- No removed obsoletes

anaconda-11.1.2.195-1 - anaconda-11.1.2.209-1

- Group: Applications/System
- Summary: Graphical system installer
- Description: The anaconda package contains the program which was used to install your system. These files are of little use on an already installed system.
- Added Dependencies:
  - pykickstart >= 0.43.8
- Removed Dependencies:
  - pykickstart
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

apr-util-1.2.7-7.el5\_3.2 - apr-util-1.2.7-11.el5

- Group: System Environment/Libraries
- Summary: Apache Portable Runtime Utility library
- Description: The mission of the Apache Portable Runtime (APR) is to provide a free library of C data structures and routines. This library contains additional utility interfaces for APR; including support for XML, LDAP, database interfaces, URI parsing and more.
- Added Dependencies:
  - mysql-devel
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

#### at-3.1.8-82.fc6 - at-3.1.8-84.el5

- Group: System Environment/Daemons
- Summary: Job spooling tools.
- Description: At and batch read commands from standard input or from a specified file. At allows you to specify that a command will be run at a particular time. Batch will execute commands when the system load levels drop to a particular level. Both commands use /bin/sh. You should install the at package if you need a utility for time-oriented job control. Note: If it is a recurring job that will need to be repeated at the same time every day/week, etc. you should use crontab instead.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

#### audit-1.7.13-2.el5 - audit-1.7.17-3.el5

- Group: System Environment/Daemons
- Summary: User space tools for 2.6 kernel auditing
- Description: The audit package contains the user space utilities for storing and searching the audit records generate by the audit subsystem in the Linux 2.6 kernel.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

autofs-5.0.1-0.rc2.131.el5 - autofs-5.0.1-0.rc2.143.el5

- Group: System Environment/Daemons
- Summary: A tool for automatically mounting and unmounting filesystems.
- Description: autofs is a daemon which automatically mounts filesystems when you use them, and unmounts them later when you are not using them. This can include network filesystems, CD-ROMs, floppies, and so forth.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

automake-1.9.6-2.1 - automake-1.9.6-2.3.el5

- Group: Development/Tools
- Summary: A GNU tool for automatically creating Makefiles.
- Description: Automake is a tool for automatically generating `Makefile.in' files compliant with the GNU Coding Standards. You should install Automake if you are developing software and would like to use its ability to automatically generate GNU standard Makefiles. If you install Automake, you will also need to install GNU's Autoconf package.
- Added Dependencies:
  - bison
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

automake14-1.4p6-13 - automake14-1.4p6-13.el5.1

- Group: Development/Tools

- Summary: A GNU tool for automatically creating Makefiles.
- Description: Automake is a tool for automatically generating `Makefile.in' files compliant with the GNU Coding Standards. This package contains Automake 1.4, an older version of Automake. You should install it if you need to run automake in a project that has not yet been updated to work with newer versions of Automake.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

#### automake15-1.5-16 - automake15-1.5-16.el5.2

- Group: Development/Tools
- Summary: A GNU tool for automatically creating Makefiles.
- Description: Automake is a tool for automatically generating `Makefile.in' files compliant with the GNU Coding Standards. This package contains Automake 1.5, an older version of Automake. You should install it if you need to run automake in a project that has not yet been updated to work with newer versions of Automake.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

#### automake16-1.6.3-8 - automake16-1.6.3-8.el5.1

- Group: Development/Tools
- Summary: A GNU tool for automatically creating Makefiles.
- Description: Automake is a tool for automatically generating `Makefile.in' files compliant with the GNU Coding Standards. This package contains Automake 1.6, an older version of Automake.

You should install it if you need to run automake in a project that has not yet been updated to work with latest version of Automake.

- Added Dependencies:
  - texinfo
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

automake17-1.7.9-7 - automake17-1.7.9-7.el5.2

- Group: Development/Tools
- Summary: A GNU tool for automatically creating Makefiles.
- Description: Automake is a tool for automatically generating `Makefile.in' files compliant with the GNU Coding Standards. This package contains Automake 1.7, an older version of Automake. You should install it if you need to run automake in a project that has not yet been updated to work with latest version of Automake.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

avahi-0.6.16-6.el5 - avahi-0.6.16-7.el5

- Group: System Environment/Base
- Summary: Local network service discovery
- Description: Avahi is a system which facilitates service discovery on a local network -- this means that you can plug your laptop or computer into a network and instantly be able to view other people who you can chat with, find printers to print to or find files being shared. This kind

of technology is already found in MacOS X (branded 'Rendezvous', 'Bonjour' and sometimes 'ZeroConf') and is very convenient.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

bind-9.3.6-4.P1.el5 - bind-9.3.6-4.P1.el5\_4.2

- Group: System Environment/Daemons
- Summary: The Berkeley Internet Name Domain (BIND) DNS (Domain Name System) server.
- Description: BIND (Berkeley Internet Name Domain) is an implementation of the DNS (Domain Name System) protocols. BIND includes a DNS server (named), which resolves host names to IP addresses; a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating properly.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

binutils-2.17.50.0.6-12.el5 - binutils-2.17.50.0.6-14.el5

- Group: Development/Tools
- Summary: A GNU collection of binary utilities.
- Description: Binutils is a collection of binary utilities, including ar (for creating, modifying and extracting from archives), as (a family of GNU assemblers), gprof (for displaying call graph profile data), ld (the GNU linker), nm (for listing symbols from object files), objcopy (for copying and translating object files), objdump (for displaying information from object files), ranlib (for generating an index for the contents of an archive), size (for listing the section sizes of an object



or archive file), strings (for listing printable strings from files), strip (for discarding symbols), and addr2line (for converting addresses to file and line).

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

bogl-0.1.18-11.2.1.e15.1 - bogl-0.1.18-13.e15

- Group: System Environment/Libraries
- Summary: A terminal program for displaying Unicode on the console.
- Description: BOGL stands for Ben's Own Graphics Library. It is a small graphics library for Linux kernel frame buffers. It supports only very simple graphics.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

bootparamd-0.17-24.devel.2.1 - bootparamd-0.17-26.e15

- Group: System Environment/Daemons
- Summary: A server process which provides boot information to diskless clients.
- Description: The bootparamd process provides bootparamd, a server process which provides the information needed by diskless clients in order for them to successfully boot. Bootparamd looks first in /etc/bootparams for an entry for that particular client; if a local bootparams file doesn't exist, it looks at the appropriate Network Information Service (NIS) map. Some network boot loaders (notably Sun's) rely on special boot server code on the server, in addition to the RARP and TFTP servers. This bootparamd server process is compatible with SunOS bootparam clients and servers which need that boot server code. You should install bootparamd if you need to provide boot information to diskless clients on your network.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

booty-0.80.6-5 - booty-0.80.6-7

- Group: System Environment/Libraries
- Summary: simple python bootloader config lib
- Description: Small python library for use with bootloader configuration by anaconda and up2date.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

brltty-3.7.2-1.fc6 - brltty-3.7.2-4.el5

- Group: System Environment/Daemons
- Summary: Braille display driver for Linux/Unix.
- Description: BRLTTY is a background process (daemon) which provides access to the Linux/ Unix console (when in text mode) for a blind person using a refreshable braille display. It drives the braille display, and provides complete screen review functionality. Some speech capability has also been incorporated.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

checkpolicy-1.33.1-4.el5 - checkpolicy-1.33.1-6.el5

- Group: Development/System
- Summary: SELinux policy compiler
- Description: Security-enhanced Linux is a feature of the Linux® kernel and a number of utilities with enhanced security functionality designed to add mandatory access controls to Linux. The Security-enhanced Linux kernel contains new architectural components originally developed to improve the security of the Flask operating system. These architectural components provide general support for the enforcement of many kinds of mandatory access control policies, including those based on the concepts of Type Enforcement®, Role-based Access Control, and Multi-level Security. This package contains checkpolicy, the SELinux policy compiler. Only required for building policies.
- Added Dependencies:
  - libsepol-devel >= 1.15.2-3
- Removed Dependencies:
  - libsepol-devel >= 1.15.2-1
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

chkconfig-1.3.30.1-2 - chkconfig-1.3.30.2-2.el5

- Group: System Environment/Base
- Summary: A system tool for maintaining the /etc/rc\*.d hierarchy.
- Description: Chkconfig is a basic system utility. It updates and queries runlevel information for system services. Chkconfig manipulates the numerous symbolic links in /etc/rc.d, to relieve system administrators of some of the drudgery of manually editing the symbolic links.
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cman-2.0.115-1.el5 - cman-2.0.115-34.el5

- Group: System Environment/Base
- Summary: cman - The Cluster Manager
- Description: cman - The Cluster Manager
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cmirror-1.1.39-2.el5 - cmirror-1.1.39-8.el5

- Group: System Environment/Base
- Summary: cmirror - The Cluster Mirror Package
- Description: cmirror - Cluster Mirroring
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cmirror-kmod-0.1.22-1.el5 - cmirror-kmod-0.1.22-3.el5

- Group: System Environment/Kernel
- Summary: cmirror kernel modules
- Description: cmirror-kmod - The Cluster Mirror kernel modules
- Added Dependencies:
  - kernel-devel-ia64 = 2.6.18-182.el5
  - kernel-xen-devel-ia64 = 2.6.18-182.el5
- Removed Dependencies:
  - kernel-devel-ia64 = 2.6.18-159.el5
  - kernel-xen-devel-ia64 = 2.6.18-159.el5
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

conga-0.12.2-6.el5 - conga-0.12.2-12.el5

- Group: System Environment/Base
- Summary: Remote Management System
- Description: Conga is a project developing management system for remote stations. It consists of luci, https frontend, and ricci, secure daemon that dispatches incoming messages to underlying management modules.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

**coolkey-1.1.0-6.el5 - coolkey-1.1.0-14.el5**

- Group: System Environment/Libraries
- Summary: CoolKey PKCS #11 module
- Description: Linux Driver support for the CoolKey and CAC products.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

**coreutils-5.97-23.el5 - coreutils-5.97-23.el5\_4.2**

- Group: System Environment/Base
- Summary: The GNU core utilities: a set of tools commonly used in shell scripts
- Description: These are the GNU core utilities. This package is the combination of the old GNU fileutils, sh-utils, and textutils packages.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

**cpio-2.6-23.el5 - cpio-2.6-23.el5\_4.1**

- Group: Applications/Archiving
- Summary: A GNU archiving program.
- Description: GNU cpio copies files into or out of a cpio or tar archive. Archives are files which contain a collection of other files plus information about them, such as their file name, owner, timestamps, and access permissions. The archive can be another file on the disk, a magnetic tape, or a pipe. GNU cpio supports the following archive formats: binary, old ASCII, new ASCII,

crc, HPUX binary, HPUX old ASCII, old tar and POSIX.1 tar. By default, cpio creates binary format archives, so that they are compatible with older cpio programs. When it is extracting files from archives, cpio automatically recognizes which kind of archive it is reading and can read archives created on machines with a different byte-order. Install cpio if you need a program to manage file archives.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cpuspeed-1.2.1-8.el5 - cpuspeed-1.2.1-9.el5

- Group: System Environment/Base
- Summary: CPU frequency adjusting daemon
- Description: cpuspeed is a daemon that dynamically changes the speed of your processor(s) depending upon its current workload if it is capable (needs Intel Speedstep, AMD PowerNow!, or similar support). This package also supports enabling cpu frequency scaling via in-kernel governors on Intel Centrino and AMD Athlon64/Opteron platforms.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

crash-4.0-8.9.1.el5 - crash-4.1.2-4.el5

- Group: Development/Debuggers
- Summary: crash utility for live systems; netdump, diskdump, kdump, LKCD or mcore dumpfiles
- Description: The core analysis suite is a self-contained tool that can be used to investigate either live systems, kernel core dumps created from the netdump, diskdump and kdump

packages from Red Hat Linux, the mcore kernel patch offered by Mission Critical Linux, or the LKCD kernel patch.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cups-1.3.7-11.el5 - cups-1.3.7-18.el5

- Group: System Environment/Daemons
- Summary: Common Unix Printing System
- Description: The Common UNIX Printing System provides a portable printing layer for UNIX® operating systems. It has been developed by Easy Software Products to promote a standard printing solution for all UNIX vendors and users. CUPS provides the System V and Berkeley command-line interfaces.
- Added Dependencies:
  - poppler-utils
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

curl-7.15.5-2.1.el5\_3.5 - curl-7.15.5-9.el5

- Group: Applications/Internet
- Summary: A utility for getting files from remote servers (FTP, HTTP, and others).
- Description: cURL is a tool for getting files from FTP, HTTP, Gopher, Telnet, and Dict servers, using any of the supported protocols. cURL is designed to work without user interaction or any kind of interactivity. cURL offers many useful capabilities, like proxy support, user authentication, FTP upload, HTTP post, and file transfer resume.



- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cyrus-imapd-2.3.7-7.el5 - cyrus-imapd-2.3.7-7.el5\_4.3

- Group: System Environment/Daemons
- Summary: A high-performance mail server with IMAP, POP3, NNTP and SIEVE support
- Description: The cyrus-imapd package contains the core of the Cyrus IMAP server. It is a scaleable enterprise mail system designed for use from small to large enterprise environments using standards-based internet mail technologies. A full Cyrus IMAP implementation allows a seamless mail and bulletin board environment to be set up across multiple servers. It differs from other IMAP server implementations in that it is run on "sealed" servers, where users are not normally permitted to log in and have no system account on the server. The mailbox database is stored in parts of the filesystem that are private to the Cyrus IMAP server. All user access to mail is through software using the IMAP, POP3 or KPOP protocols. It also includes support for virtual domains, NNTP, mailbox annotations, and much more. The private mailbox database design gives the server large advantages in efficiency, scalability and administratability. Multiple concurrent read/write connections to the same mailbox are permitted. The server supports access control lists on mailboxes and storage quotas on mailbox hierarchies. The Cyrus IMAP server supports the IMAP4rev1 protocol described in RFC 3501. IMAP4rev1 has been approved as a proposed standard. It supports any authentication mechanism available from the SASL library, imaps/pop3s/nntps (IMAP/POP3/NNTP encrypted using SSL and TLSv1) can be used for security. The server supports single instance store where possible when an email message is addressed to multiple recipients, SIEVE provides server side email filtering.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

## cyrus-sasl-2.1.22-5.el5 - cyrus-sasl-2.1.22-5.el5\_4.3

- Group: System Environment/Libraries
- Summary: The Cyrus SASL library.
- Description: The cyrus-sasl package contains the Cyrus implementation of SASL. SASL is the Simple Authentication and Security Layer, a method for adding authentication support to connection-based protocols.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

## dapl-2.0.19-2.el5 - dapl-2.0.25-2.el5

- Group: System Environment/Libraries
- Summary: Library providing access to the DAT 1.2 and 2.0 APIs
- Description: libdat and libdapl provide a userspace implementation of the DAT 1.2 and 2.0 API that is built to natively support InfiniBand/iWARP network technology.
- Added Dependencies:
  - libibverbs-devel >= 1.1.3
  - librdmacm-devel >= 1.0.10
- Removed Dependencies:
  - libibverbs-devel >= 1.1.2-4
  - librdmacm-devel >= 1.0.8-5
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

## Appendix A. Package Manifest

---

dbus-1.1.2-12.el5 - dbus-1.1.2-14.el5

- Group: System Environment/Libraries
- Summary: D-BUS message bus
- Description: D-BUS is a system for sending messages between applications. It is used both for the systemwide message bus service, and as a per-user-login-session messaging facility.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dbus-python-0.70-7.el5 - dbus-python-0.70-9.el5\_4

- Group: System Environment/Libraries
- Summary: D-Bus Python Bindings
- Description: D-Bus python bindings for use with python programs.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

device-mapper-1.02.32-1.el5 - device-mapper-1.02.39-1.el5

- Group: System Environment/Base
- Summary: device mapper library
- Description: This package contains the supporting userspace files (libdevmapper and dmsetup) for the device-mapper.
- No added dependencies

- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

device-mapper-multipath-0.4.7-30.el5 - device-mapper-multipath-0.4.7-34.el5

- Group: System Environment/Base
- Summary: Tools to manage multipath devices using device-mapper.
- Description: device-mapper-multipath provides tools to manage multipath devices by instructing the device-mapper multipath kernel module what to do. The tools are : \* multipath : Scan the system for multipath devices and assemble them. \* multipathd : Detects when paths fail and execs multipath to update things.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dhcp-3.0.5-21.el5 - dhcp-3.0.5-23.el5

- Group: System Environment/Daemons
- Summary: DHCP (Dynamic Host Configuration Protocol) server and relay agent.
- Description: DHCP (Dynamic Host Configuration Protocol) is a protocol which allows individual devices on an IP network to get their own network configuration information (IP address, subnetmask, broadcast address, etc.) from a DHCP server. The overall purpose of DHCP is to make it easier to administer a large network. The dhcp package includes the ISC DHCP service and relay agent. To use DHCP on your network, install a DHCP service (or relay agent), and on clients run a DHCP client daemon. The dhcp package provides the ISC DHCP service and relay agent.
- No added dependencies
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dhcpv6-1.0.10-17.el5 - dhcpv6-1.0.10-18.el5

- Group: System Environment/Daemons
- Summary: DHCPv6 - DHCP server and client for IPv6
- Description: Implements the Dynamic Host Configuration Protocol (DHCP) for Internet Protocol version 6 (IPv6) networks in accordance with RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6). Consists of dhcp6s(8), the server DHCP daemon, and dhcp6r(8), the DHCPv6 relay agent. Install this package if you want to support dynamic configuration of IPv6 addresses and parameters on your IPv6 network.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dmidecode-2.9-1.el5 - dmidecode-2.10-3.el5

- Group: System Environment/Base
- Summary: Tool to analyse BIOS DMI data.
- Description: dmidecode reports information about x86 hardware as described in the system BIOS according to the SMBIOS/DMI standard. This information typically includes system manufacturer, model name, serial number, BIOS version, asset tag as well as a lot of other details of varying level of interest and reliability depending on the manufacturer. This will often include usage status for the CPU sockets, expansion slots (e.g. AGP, PCI, ISA) and memory module slots, and the list of I/O ports (e.g. serial, parallel, USB).
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dmraid-1.0.0.rc13-53.el5 - dmraid-1.0.0.rc13-63.el5

- Group: System Environment/Base
- Summary: dmraid (Device-mapper RAID tool and library)
- Description: DMRAID supports RAID device discovery, RAID set activation and display of properties for ATARAID on Linux >= 2.4 using device-mapper.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dnsmasq-2.45-1.el5\_2.1 - dnsmasq-2.45-1.1.el5\_3

- Group: System Environment/Daemons
- Summary: A lightweight DHCP/caching DNS server
- Description: Dnsmasq is lightweight, easy to configure DNS forwarder and DHCP server. It is designed to provide DNS and, optionally, DHCP, to a small network. It can serve the names of local machines which are not in the global DNS. The DHCP server integrates with the DNS server and allows machines with DHCP-allocated addresses to appear in the DNS with names configured either in each host or in a central configuration file. Dnsmasq supports static and dynamic DHCP leases and BOOTP for network booting of diskless machines.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

## Appendix A. Package Manifest

---

- No added obsoletes
- No removed obsoletes

dogtail-0.6.1-2.el5 - dogtail-0.6.1-3.el5

- Group: User Interface/X
- Summary: GUI test tool and automation framework
- Description: GUI test tool and automation framework that uses assistive technologies to communicate with desktop applications.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dosfstools-2.11-7.el5 - dosfstools-2.11-9.el5

- Group: Applications/System
- Summary: Utilities for making and checking MS-DOS FAT filesystems on Linux
- Description: The dosfstools package includes the mkdosfs and dosfsck utilities, which respectively make and check MS-DOS FAT filesystems on hard drives or on floppies.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dstat-0.6.6-3.el5 - dstat-0.6.6-3.el5\_4.1

- Group: System Environment/Base
- Summary: Versatile resource statistics tool

- Description: Dstat is a versatile replacement for vmstat, iostat, netstat and ifstat. Dstat overcomes some of their limitations and adds some extra features, more counters and flexibility. Dstat is handy for monitoring systems during performance tuning tests, benchmarks or troubleshooting. Dstat allows you to view all of your system resources instantly, you can eg. compare disk usage in combination with interrupts from your IDE controller, or compare the network bandwidth numbers directly with the disk throughput (in the same interval). Dstat gives you detailed selective information in columns and clearly indicates in what magnitude and unit the output is displayed. Less confusion, less mistakes.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

#### e4fsprogs-1.41.5-3.el5 - e4fsprogs-1.41.9-3.el5

- Group: System Environment/Base
- Summary: Utilities for managing the fourth extended (ext4) filesystem
- Description: The e4fsprogs package contains a number of utilities for creating, checking, modifying, and correcting any inconsistencies in the fourth extended (ext4) filesystem. E4fsprogs contains e4fsck (used to repair filesystem inconsistencies after an unclean shutdown), mke4fs (used to initialize a partition to contain an empty ext4 filesystem), debugfs (used to examine the internal structure of a filesystem, to manually repair a corrupted filesystem, or to create test cases for e4fsck), tune4fs (used to modify filesystem parameters), and most of the other core ext4fs filesystem utilities. Please note that "e4fsprogs" simply contains renamed static binaries from the equivalent upstream e2fsprogs release; it is packaged this way for Red Hat Enterprise Linux 5 to ensure that the many changes included for ext4 do not destabilize the core e2fsprogs in RHEL5. You should install the e4fsprogs package if you need to manage the performance of an ext4 filesystem.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes



## Appendix A. Package Manifest

---

- No removed obsoletes

elilo-3.6-3 - elilo-3.6-4

- Group: System Environment/Base
- Summary: ELILO linux boot loader for EFI-based systems
- Description: ELILO is a linux boot loader for EFI-based systems, such as IA-64.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

elinks-0.11.1-5.1.0.1.el5 - elinks-0.11.1-6.el5\_4.1

- Group: Applications/Internet
- Summary: A text-mode Web browser.
- Description: Links is a text-based Web browser. Links does not display any images, but it does support frames, tables and most other HTML tags. Links' advantage over graphical browsers is its speed--Links starts and exits quickly and swiftly displays Web pages.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

esc-1.1.0-9.el5 - esc-1.1.0-11.el5

- Group: Applications/Internet
- Summary: Enterprise Security Client Smart Card Client
- Description: Enterprise Security Client allows the user to enroll and manage their cryptographic smartcards.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

etherboot-5.4.4-10.el5 - etherboot-5.4.4-13.el5

- Group: Development/Tools
- Summary: Etherboot collection of boot roms
- Description: Etherboot is a software package for creating ROM images that can download code over an Ethernet network to be executed on an x86 computer. Many network adapters have a socket where a ROM chip can be installed. Etherboot is code that can be put in such a ROM
- Added Dependencies:
  - /usr/include/gnu/stubs-32.h
- Removed Dependencies:
  - glibc32
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ethtool-6-3.el5 - ethtool-6-4.el5

- Group: Applications/System
- Summary: Ethernet settings tool for PCI ethernet cards
- Description: This utility allows querying and changing of ethernet card settings, such as speed, port, autonegotiation, and PCI locations.
- No added dependencies
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

evince-0.6.0-9.el5 - evince-0.6.0-13.el5

- Group: Applications/Publishing
- Summary: Document viewer
- Description: evince is a GNOME-based document viewer.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

exim-4.63-3.el5 - exim-4.63-5.el5

- Group: System Environment/Daemons
- Summary: The exim mail transfer agent
- Description: Exim is a message transfer agent (MTA) developed at the University of Cambridge for use on Unix systems connected to the Internet. It is freely available under the terms of the GNU General Public Licence. In style it is similar to Smail 3, but its facilities are more general. There is a great deal of flexibility in the way mail can be routed, and there are extensive facilities for checking incoming mail. Exim can be installed in place of sendmail, although the configuration of exim is quite different to that of sendmail.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

expat-1.95.8-8.2.1 - expat-1.95.8-8.3.el5\_4.2

- Group: System Environment/Libraries
- Summary: A library for parsing XML.
- Description: This is expat, the C library for parsing XML, written by James Clark. Expat is a stream oriented XML parser. This means that you register handlers with the parser prior to starting the parse. These handlers are called when the parser discovers the associated structures in the document being parsed. A start tag is an example of the kind of structures for which you may register handlers.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

fetchmail-6.3.6-1.1.el5 - fetchmail-6.3.6-1.1.el5\_3.1

- Group: Applications/Internet
- Summary: A remote mail retrieval and forwarding utility
- Description: Fetchmail is a remote mail retrieval and forwarding utility intended for use over on-demand TCP/IP links, like SLIP or PPP connections. Fetchmail supports every remote-mail protocol currently in use on the Internet (POP2, POP3, RPOP, APOP, KPOP, all IMAPs, ESMTP ETRN, IPv6, and IPSEC) for retrieval. Then Fetchmail forwards the mail through SMTP so you can read it through your favorite mail client. Install fetchmail if you need to retrieve mail over SLIP or PPP connections.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

## Appendix A. Package Manifest

---

- No added obsoletes
- No removed obsoletes

filesystem-2.4.0-2 - filesystem-2.4.0-3.el5

- Group: System Environment/Base
- Summary: The basic directory layout for a Linux system.
- Description: The filesystem package is one of the basic packages that is installed on a Red Hat Linux system. Filesystem contains the basic directory layout for a Linux operating system, including the correct permissions for the directories.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

firefox-3.0.12-1.el5\_3 - firefox-3.0.18-1.el5\_4

- Group: Applications/Internet
- Summary: Mozilla Firefox Web browser
- Description: Mozilla Firefox is an open-source web browser, designed for standards compliance, performance and portability.
- Added Dependencies:
  - xulrunner-devel >= 1.9.0.18-1
  - xulrunner-devel-unstable >= 1.9.0.18-1
- Removed Dependencies:
  - xulrunner-devel >= 1.9.0.12-1
  - xulrunner-devel-unstable >= 1.9.0.12-1
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

firstboot-1.4.27.7-1.el5 - firstboot-1.4.27.8-1.el5

- Group: System Environment/Base
- Summary: Initial system configuration utility
- Description: The firstboot utility runs after installation. It guides the user through a series of steps that allows for easier configuration of the machine.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

freeradius-1.1.3-1.4.el5 - freeradius-1.1.3-1.6.el5

- Group: System Environment/Daemons
- Summary: High-performance and highly configurable free RADIUS server.
- Description: The FreeRADIUS Server Project is a high performance and highly configurable GPL'd free RADIUS server. The server is similar in some respects to Livingston's 2.0 server. While FreeRADIUS started as a variant of the Cistron RADIUS server, they don't share a lot in common any more. It now has many more features than Cistron or Livingston, and is much more configurable. FreeRADIUS is an Internet authentication daemon, which implements the RADIUS protocol, as defined in RFC 2865 (and others). It allows Network Access Servers (NAS boxes) to perform authentication for dial-up users. There are also RADIUS clients available for Web servers, firewalls, Unix logins, and more. Using RADIUS allows authentication and authorization for a network to be centralized, and minimizes the amount of re-configuration which has to be done when adding or deleting new users.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

## Appendix A. Package Manifest

---

- No added obsoletes
- No removed obsoletes

gail-1.9.2-1.fc6 - gail-1.9.2-3.el5

- Group: System Environment/Libraries
- Summary: Accessibility implementation for GTK+ and GNOME libraries
- Description: GAIL implements the abstract interfaces found in ATK for GTK+ and GNOME libraries, enabling accessibility technologies such as at-spi to access those GUIs.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gcc-4.1.2-46.el5 - gcc-4.1.2-48.el5

- Group: Development/Languages
- Summary: Various compilers (C, C++, Objective-C, Java, ...)
- Description: The gcc package contains the GNU Compiler Collection version 4.1. You'll need this package in order to compile C code.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gd-2.0.33-9.4.el5\_1.1 - gd-2.0.33-9.4.el5\_4.2

- Group: System Environment/Libraries
- Summary: A graphics library for quick creation of PNG or JPEG images

- Description: The gd graphics library allows your code to quickly draw images complete with lines, arcs, text, multiple colors, cut and paste from other images, and flood fills, and to write out the result as a PNG or JPEG file. This is particularly useful in Web applications, where PNG and JPEG are two of the formats accepted for inline images by most browsers. Note that gd is not a paint program.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

#### gdb-6.8-37.el5 - gdb-7.0.1-23.el5

- Group: Development/Debuggers
- Summary: A GNU source-level debugger for C, C++, Java and other languages
- Description: GDB, the GNU debugger, allows you to debug programs written in C, C++, Java, and other languages, by executing them in a controlled fashion and printing their data.
- Added Dependencies:
  - zlib-devel
- Removed Dependencies:
  - dejagnu
  - gcc
  - glibc-devel
  - gzip
  - make
  - prelink
  - sharutils
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts



## Appendix A. Package Manifest

---

- No added obsoletes
- No removed obsoletes

gfs-kmod-0.1.34-2.el5 - gfs-kmod-0.1.34-12.el5

- Group: System Environment/Kernel
- Summary: gfs kernel modules
- Description: gfs - The Global File System is a symmetric, shared-disk, cluster file system.
- Added Dependencies:
  - kernel-devel-ia64 = 2.6.18-192.el5
  - kernel-xen-devel-ia64 = 2.6.18-192.el5
- Removed Dependencies:
  - kernel-devel-ia64 = 2.6.18-159.el5
  - kernel-xen-devel-ia64 = 2.6.18-159.el5
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gfs-utils-0.1.20-1.el5 - gfs-utils-0.1.20-7.el5

- Group: System Environment/Kernel
- Summary: Utilities for managing the global filesystem (GFS)
- Description: The gfs-utils package contains a number of utilities for creating, checking, modifying, and correcting any inconsistencies in GFS filesystems.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

gfs2-utils-0.1.62-1.el5 - gfs2-utils-0.1.62-20.el5

- Group: System Environment/Kernel
- Summary: Utilities for managing the global filesystem (GFS)
- Description: The gfs2-utils package contains a number of utilities for creating, checking, modifying, and correcting any inconsistencies in GFS filesystems.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

glibc-2.5-42 - glibc-2.5-49

- Group: System Environment/Libraries
- Summary: The GNU libc libraries.
- Description: The glibc package contains standard libraries which are used by multiple programs on the system. In order to save disk space and memory, as well as to make upgrading easier, common system code is kept in one place and shared between programs. This particular package contains the most important sets of shared libraries: the standard C library and the standard math library. Without these two libraries, a Linux system will not function.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gnome-vfs2-2.16.2-4.el5 - gnome-vfs2-2.16.2-6.el5

- Group: System Environment/Libraries

- Summary: The GNOME virtual file-system libraries
- Description: GNOME VFS is the GNOME virtual file system. It is the foundation of the Nautilus file manager. It provides a modular architecture and ships with several modules that implement support for file systems, http, ftp, and others. It provides a URI-based API, backend supporting asynchronous file operations, a MIME type manipulation library, and other features.
- Added Dependencies:
  - libsmbclient-devel
- Removed Dependencies:
  - samba-common >= 3.0.8-0.pre1.3
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

### gnutls-1.4.1-3.el5\_2.1 - gnutls-1.4.1-3.el5\_3.5

- Group: System Environment/Libraries
- Summary: A TLS protocol implementation.
- Description: GnuTLS is a project that aims to develop a library which provides a secure layer, over a reliable transport layer. Currently the GnuTLS library implements the proposed standards by the IETF's TLS working group.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

### gpart-0.1h-3.1 - gpart-0.1h-5.el5

- Group: Applications/System
- Summary: A program for recovering corrupt partition tables

- Description: Gpart is a small tool which tries to guess what partitions are on a PC type harddisk in case the primary partition table was damaged.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

#### gzip-1.3.5-10.el5 - gzip-1.3.5-11.el5\_4.1

- Group: Applications/File
- Summary: The GNU data compression program.
- Description: The gzip package contains the popular GNU gzip data compression program. Gzipped files have a .gz extension. Gzip should be installed on your Red Hat Linux system, because it is a very commonly used data compression program.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

#### hal-0.5.8.1-52.el5 - hal-0.5.8.1-59.el5

- Group: System Environment/Libraries
- Summary: Hardware Abstraction Layer
- Description: HAL is daemon for collection and maintaining information from several sources about the hardware on the system. It provides a live device list through D-BUS.
- No added dependencies
- No removed dependencies
- No added provides

## Appendix A. Package Manifest

---

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

### hmaccalc-0.9.6-1.el5 - hmaccalc-0.9.6-3.el5

- Group: System Environment/Base
- Summary: Tools for computing and checking HMAC values for files
- Description: The hmaccalc package contains tools which can calculate HMAC (hash-based message authentication code) values for files. The names and interfaces are meant to mimic the sha\*sum tools provided by the coreutils package.
- Added Dependencies:
  - autoconf
  - automake
  - prelink
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

### httpd-2.2.3-31.el5 - httpd-2.2.3-43.el5

- Group: System Environment/Daemons
- Summary: Apache HTTP Server
- Description: The Apache HTTP Server is a powerful, efficient, and extensible web server.
- Added Dependencies:
  - openssl-devel >= 0.9.8e-12.el5\_4.4
- Removed Dependencies:
  - openssl-devel
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

hwdata-0.213.16-1.el5 - hwdata-0.213.18-1.el5.1

- Group: System Environment/Base
- Summary: Hardware identification and configuration data
- Description: hwdata contains various hardware identification and configuration data, such as the pci.ids database and MonitorsDb databases.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

iasl-20061109-5.el5 - iasl-20090123-1.el5

- Group: Development/Languages
- Summary: Intel ASL compiler/decompiler
- Description: iasl compiles ASL (ACPI Source Language) into AML (ACPI Machine Language), which is suitable for inclusion as a DSDT in system firmware. It also can disassemble AML, for debugging purposes.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

## Appendix A. Package Manifest

---

- No removed obsoletes

ibsim-0.5-1.el5 - ibsim-0.5-2.el5

- Group: System Environment/Libraries
- Summary: InfiniBand fabric simulator for management
- Description: ibsim provides simulation of infiniband fabric for using with OFA OpenSM, diagnostic and management tools.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ibutils-1.2-10.el5 - ibutils-1.2-11.el5

- Group: System Environment/Libraries
- Summary: OpenIB Mellanox InfiniBand Diagnostic Tools
- Description: ibutils provides IB network and path diagnostics.
- Added Dependencies:
  - opensm-devel >= 3.3.0
- Removed Dependencies:
  - opensm-devel >= 3.2.0
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

infiniband-diags-1.4.4-1.el5 - infiniband-diags-1.5.3-1.el5

- Group: System Environment/Libraries
- Summary: OpenFabrics Alliance InfiniBand Diagnostic Tools

- Description: This package provides IB diagnostic programs and scripts needed to diagnose an IB subnet.
- Added Dependencies:
  - opensm-devel >= 3.3.0
- Removed Dependencies:
  - libibcommon-devel
  - opensm-devel >= 3.2.0
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

#### inn-2.4.3-8.el5 - inn-2.4.3-9.el5

- Group: System Environment/Daemons
- Summary: The InterNetNews (INN) system, an Usenet news server.
- Description: INN (InterNetNews) is a complete system for serving Usenet news and/or private newsfeeds. INN includes innd, an NNTP (NetNews Transport Protocol) server, and nnrpd, a newsreader that is spawned for each client. Both innd and nnrpd vary slightly from the NNTP protocol, but not in ways that are easily noticed. Install the inn package if you need a complete system for serving and reading Usenet news. You may also need to install inn-devel, if you are going to use a separate program which interfaces to INN, like newsgate or tin.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

#### iproute-2.6.18-10.el5 - iproute-2.6.18-11.el5

- Group: Applications/System
- Summary: Advanced IP routing and network device configuration tools.



## Appendix A. Package Manifest

---

- Description: The iproute package contains networking utilities (ip and rtmon, for example) which are designed to use the advanced networking capabilities of the Linux 2.4.x and 2.6.x kernel.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

iprutils-2.2.13-1.el5 - iprutils-2.2.18-1.el5

- Group: System Environment/Base
- Summary: Utilities for the IBM Power Linux RAID adapters
- Description: Provides a suite of utilities to manage and configure SCSI devices supported by the ipr SCSI storage device driver.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

iptables-1.3.5-5.3.el5 - iptables-1.3.5-5.3.el5\_4.1

- Group: System Environment/Base
- Summary: Tools for managing Linux kernel packet filtering capabilities.
- Description: The iptables utility controls the network packet filtering code in the Linux kernel. If you need to set up firewalls and/or IP masquerading, you should install this package.
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

#### iptstate-1.4-1.1.2.2 - iptstate-1.4-2.el5

- Group: System Environment/Base
- Summary: A top-like display of IP Tables state table entries
- Description: IP Tables State (iptstate) was originally written to implement the "state top" feature of IP Filter (see "The Idea" below) in IP Tables. "State top" displays the states held by your stateful firewall in a top-like manner. Since IP Tables doesn't have a built in way to easily display this information even once, an option was added to just have it display the state table once. Features include: - Top-like realtime state table information - Sorting by any field - Reversible sorting - Single display of state table - Customizable refresh rate - Open Source (specifically I'm using the zlib license)
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

#### iscsi-initiator-utils-6.2.0.871-0.10.el5 - iscsi-initiator-utils-6.2.0.871-0.16.el5

- Group: System Environment/Daemons
- Summary: iSCSI daemon and utility programs
- Description: The iscsi package provides the server daemon for the iSCSI protocol, as well as the utility programs used to manage it. iSCSI is a protocol for distributed disk access using SCSI commands sent over Internet Protocol networks.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

## Appendix A. Package Manifest

---

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

java-1.6.0-openjdk-1.6.0.0-1.2.b09.el5 - java-1.6.0-openjdk-1.6.0.0-1.7.b09.el5

- Group: Development/Languages
- Summary: OpenJDK Runtime Environment
- Description: The OpenJDK runtime environment.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

kdegraphics-3.5.4-13.el5\_3 - kdegraphics-3.5.4-15.el5\_4.2

- Group: Applications/Multimedia
- Summary: K Desktop Environment - Graphics Applications
- Description: Graphics applications for the K Desktop Environment. Includes: kdvi (displays TeX .dvi files) kghostview (displays postscript files) kcoloredit (palette editor and color chooser) kiconedit (icon editor) kolourpaint (a simple drawing program) ksnapshot (screen capture utility) kview (image viewer for GIF, JPEG, TIFF, etc.) kooka (scanner application) kruler (screen ruler and color measurement tool) kpdf (display pdf files)
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

## kdelibs-3.5.4-22.el5\_3 - kdelibs-3.5.4-25.el5\_4.1

- Group: System Environment/Libraries
- Summary: K Desktop Environment - Libraries
- Description: Libraries for the K Desktop Environment: KDE Libraries included: kdecopre (KDE core library), kdeui (user interface), kfm (file manager), khtmlw (HTML widget), kio (Input/Output, networking), kspell (spelling checker), jscript (javascript), kab (addressbook), kimgio (image manipulation).
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

## kernel-2.6.18-164.el5 - kernel-2.6.18-194.el5

- Group: System Environment/Kernel
- Summary: The Linux kernel (the core of the Linux operating system)
- Description: The kernel package contains the Linux kernel (vmlinuz), the core of any Linux operating system. The kernel handles the basic functions of the operating system: memory allocation, process allocation, device input and output, etc.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

## kexec-tools-1.102pre-77.el5 - kexec-tools-1.102pre-96.el5

- Group: Applications/System
- Summary: The kexec/kdump userspace component.

## Appendix A. Package Manifest

---

- Description: kexec-tools provides /sbin/kexec binary that facilitates a new kernel to boot using the kernel's kexec feature either on a normal or a panic reboot. This package contains the /sbin/kexec binary and ancillary utilities that together form the userspace component of the kernel's kexec feature.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

krb5-1.6.1-36.el5 - krb5-1.6.1-36.el5\_4.1

- Group: System Environment/Libraries
- Summary: The Kerberos network authentication system.
- Description: Kerberos V5 is a trusted-third-party network authentication system, which can improve your network's security by eliminating the insecure practice of cleartext passwords.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ksh-20080202-14.el5 - ksh-20100202-1.el5

- Group: Applications/Shells
- Summary: The Original ATT Korn Shell
- Description: KSH-93 is the most recent version of the KornShell by David Korn of AT&T Bell Laboratories. KornShell is a shell programming language, which is upward compatible with "sh" (the Bourne Shell).
- No added dependencies
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ktune-0.2-3.el5 - ktune-0.2-6.el5

- Group: System Environment/Base
- Summary: Server performance tuning service
- Description: ktune provides settings for server performance tuning. Please have a look at `/etc/sysconfig/ktune` and `/etc/sysctl.ktune` for tuning parameters.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

kudzu-1.2.57.1.21-1 - kudzu-1.2.57.1.24-1

- Group: Applications/System
- Summary: The Red Hat Linux hardware probing tool.
- Description: Kudzu is a hardware probing tool run at system boot time to determine what hardware has been added or removed from the system.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

kvm-83-105.el5 - kvm-83-164.el5

- Group: Development/Tools
- Summary: Kernel-based Virtual Machine
- Description: KVM (for Kernel-based Virtual Machine) is a full virtualization solution for Linux on x86 hardware. Using KVM, one can run multiple virtual machines running unmodified Linux or Windows images. Each virtual machine has private virtualized hardware: a network card, disk, graphics adapter, etc.
- Added Dependencies:
  - kernel-devel-x86\_64 = 2.6.18-191.el5
- Removed Dependencies:
  - kernel-devel-x86\_64 = 2.6.18-160.el5
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

less-394-6.el5 - less-436-2.el5

- Group: Applications/Text
- Summary: A text file browser similar to more, but better.
- Description: The less utility is a text file browser that resembles more, but has more capabilities. Less allows you to move backwards in the file as well as forwards. Since less doesn't have to read the entire input file before it starts, less starts up more quickly than text editors (for example, vi). You should install less because it is a basic utility for viewing text files, and you'll use it frequently.
- Added Dependencies:
  - autoconf
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

**libXi-1.0.1-3.1 - libXi-1.0.1-4.el5\_4**

- Group: System Environment/Libraries
- Summary: X.Org X11 libXi runtime library
- Description: X.Org X11 libXi runtime library
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

**libXrandr-1.1.1-3.1 - libXrandr-1.1.1-3.3**

- Group: System Environment/Libraries
- Summary: X.Org X11 libXrandr runtime library
- Description: X.Org X11 libXrandr runtime library
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

**libXt-1.0.2-3.1.fc6 - libXt-1.0.2-3.2.el5**

- Group: System Environment/Libraries
- Summary: X.Org X11 libXt runtime library
- Description: X.Org X11 libXt runtime library



- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libaio-0.3.106-3.2 - libaio-0.3.106-5

- Group: System Environment/Libraries
- Summary: Linux-native asynchronous I/O access library
- Description: The Linux-native asynchronous I/O facility ("async I/O", or "aio") has a richer API and capability set than the simple POSIX async I/O facility. This library, libaio, provides the Linux-native API for async I/O. The POSIX async I/O facility requires this library in order to provide kernel-accelerated async I/O capabilities, as do applications which require the Linux-native async I/O API.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libcmptutil-0.4-2.el5 - libcmptutil-0.5.1-1.el5

- Group: System Environment/Libraries
- Summary: CMPI Utility Library
- Description: Libcmptutil is a library of utility functions for CMPI providers. The goal is to reduce the amount of repetitive work done in most CMPI providers by encapsulating common procedures with more "normal" APIs. This extends from operations like getting typed instance properties to standardizing method dispatch and argument checking.
- No added dependencies
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libcxgb3-1.2.3-1.el5 - libcxgb3-1.2.5-2.el5

- Group: System Environment/Libraries
- Summary: Chelsio T3 iWARP HCA Userspace Driver
- Description: Userspace hardware driver for use with the libibverbs InfiniBand/iWARP verbs library. This driver enables Chelsio iWARP capable ethernet devices.
- Added Dependencies:
  - libibverbs-devel >= 1.1.3
- Removed Dependencies:
  - libibverbs-devel >= 1.1.2-4.el5
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libehca-1.2.1-3.el5 - libehca-1.2.1-6.el5

- Group: System Environment/Libraries
- Summary: IBM InfiniBand HCA Userspace Driver
- Description: IBM hardware driver for use with libibverbs user space verbs access library.
- Added Dependencies:
  - autoconf
  - libibverbs-devel >= 1.1.3
  - libtool
- Removed Dependencies:

- libibverbs-devel >= 1.1.2-4
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

### libevent-1.1a-3.2.1 - libevent-1.4.13-1

- Group: System Environment/Libraries
- Summary: Abstract asynchronous event notification library
- Description: The libevent API provides a mechanism to execute a callback function when a specific event occurs on a file descriptor or after a timeout has been reached. libevent is meant to replace the asynchronous event loop found in event driven network servers. An application just needs to call `event_dispatch()` and can then add or remove events dynamically without having to change the event loop.
- Added Dependencies:
  - doxygen
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

### libgnomecups-0.2.2-8 - libgnomecups-0.2.2-9

- Group: Development/Libraries
- Summary: GNOME library for CUPS integration
- Description: GNOME library for CUPS integration
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libgtop2-2.14.4-3.el5 - libgtop2-2.14.4-8.el5\_4

- Group: System Environment/Libraries
- Summary: libgtop library (version 2)
- Description: libgtop is a library for portably obtaining information about processes, such as their PID, memory usage, etc.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libhugetlbfs-1.3-3.el5 - libhugetlbfs-1.3-7.el5

- Group: System Environment/Libraries
- Summary: Library to access the Huge TLB Filesystem
- Description: The libhugetlbfs library interacts with the Linux hugetlbfs to make large pages available to applications in a transparent manner.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

## Appendix A. Package Manifest

---

libibcm-1.0.4-3.el5 - libibcm-1.0.5-1.el5

- Group: System Environment/Libraries
- Summary: Userspace InfiniBand Communication Manager.
- Description: libibcm provides a userspace InfiniBand Communication Management library.
- Added Dependencies:
  - libibverbs-devel >= 1.1.3
- Removed Dependencies:
  - libibverbs-devel >= 1.1.2-4.el5
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libibcommon-1.1.2-1.el5 - libibcommon-1.2.0-1.el5

- Group: System Environment/Libraries
- Summary: OpenFabrics Alliance InfiniBand management common library
- Description: libibcommon provides common utility functions for the OFA diagnostic and management tools.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libibmad-1.2.3-1.el5 - libibmad-1.3.3-1.el5

- Group: System Environment/Libraries
- Summary: OpenFabrics Alliance InfiniBand MAD library

- Description: libibmad provides low layer IB functions for use by the IB diagnostic and management programs. These include MAD, SA, SMP, and other basic IB functions.
- Added Dependencies:
  - libibumad-devel = 1.3.3
- Removed Dependencies:
  - libibumad-devel >= 1.2.3
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

#### libibumad-1.2.3-1.el5 - libibumad-1.3.3-1.el5

- Group: System Environment/Libraries
- Summary: OpenFabrics Alliance InfiniBand umad (user MAD) library
- Description: libibumad provides the user MAD library functions which sit on top of the user MAD modules in the kernel. These are used by the IB diagnostic and management tools, including OpenSM.
- No added dependencies
- Removed Dependencies:
  - libibcommon-devel >= 1.1.2
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

#### libibverbs-1.1.2-4.el5 - libibverbs-1.1.3-2.el5

- Group: System Environment/Libraries
- Summary: Library providing access to InfiniBand/iWARP hardware verbs protocol
- Description: libibverbs is a library that allows userspace processes to use InfiniBand/iWARP "verbs" as described in the InfiniBand Architecture Specification. This includes direct hardware

access for fast path operations. For this library to be useful, a device-specific plug-in module should also be installed.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libipathverbs-1.1-14.el5 - libipathverbs-1.2-2.el5

- Group: System Environment/Libraries
- Summary: QLogic InfiniPath HCA Userspace Driver
- Description: QLogic hardware driver for use with libibverbs user space verbs access library. This driver supports QLogic InfiniPath based cards.
- Added Dependencies:
  - libibverbs-devel >= 1.1.3
- Removed Dependencies:
  - libibverbs-devel >= 1.1.2-4.el5
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libmlx4-1.0.1-2.el5 - libmlx4-1.0.1-5.el5

- Group: System Environment/Libraries
- Summary: Mellanox ConnectX InfiniBand HCA Userspace Driver
- Description: Mellanox hardware driver for use with libibverbs user space verbs access library. This driver supports Mellanox ConnectX architecture cards.
- Added Dependencies:

- libibverbs-devel >= 1.1.3
- Removed Dependencies:
  - libibverbs-devel >= 1.1.2-4.el5
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

#### libmthca-1.0.5-4.el5 - libmthca-1.0.5-6.el5

- Group: System Environment/Libraries
- Summary: Mellanox InfiniBand HCA Userspace Driver
- Description: Mellanox hardware driver for use with libibverbs user space verbs access library. This driver supports Mellanox based Single Data Rate and Dual Data Rate cards, including those from Cisco, Topspin, and Voltaire. It does not support the Connect-X architecture based Quad Data Rate cards (libmlx4 handles that hardware).
- Added Dependencies:
  - libibverbs-devel >= 1.1.3
- Removed Dependencies:
  - libibverbs-devel >= 1.1.2-4.el5
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

#### libnes-0.6-2.el5 - libnes-0.9.0-2.el5

- Group: System Environment/Libraries
- Summary: NetEffect RNIC Userspace Driver
- Description: Userspace hardware driver for use with the libibverbs InfiniBand/iWARP verbs library. This driver enables NetEffect iWARP capable ethernet devices.



- Added Dependencies:
  - libibverbs-devel >= 1.1.3
- Removed Dependencies:
  - libibverbs-devel >= 1.1.2-4.el5
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

librdmacm-1.0.8-5.el5 - librdmacm-1.0.10-1.el5

- Group: System Environment/Libraries
- Summary: Userspace RDMA Connection Manager.
- Description: librdmacm provides a userspace RDMA Communication Management API.
- Added Dependencies:
  - libibverbs-devel >= 1.1.3
- Removed Dependencies:
  - libibverbs-devel >= 1.1.2-4.el5
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libsepol-1.15.2-2.el5 - libsepol-1.15.2-3.el5

- Group: System Environment/Libraries
- Summary: SELinux binary policy manipulation library
- Description: Security-enhanced Linux is a feature of the Linux® kernel and a number of utilities with enhanced security functionality designed to add mandatory access controls to Linux. The Security-enhanced Linux kernel contains new architectural components originally developed to improve the security of the Flask operating system. These architectural components provide general support for the enforcement of many kinds of mandatory access control policies,

---

including those based on the concepts of Type Enforcement®, Role-based Access Control, and Multi-level Security. libsepol provides an API for the manipulation of SELinux binary policies. It is used by checkpolicy (the policy compiler) and similar tools, as well as by programs like load\_policy that need to perform specific transformations on binary policies such as customizing policy boolean settings.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

#### libtool-1.5.22-6.1 - libtool-1.5.22-7.el5\_4

- Group: Development/Tools
- Summary: The GNU Portable Library Tool
- Description: GNU Libtool is a set of shell scripts which automatically configure UNIX and UNIX-like systems to generically build shared libraries. Libtool provides a consistent, portable interface which simplifies the process of using shared libraries. If you are developing programs which will use shared libraries, but do not use the rest of the GNU Autotools (such as GNU Autoconf and GNU Automake), you should install the libtool package. The libtool package also includes all files needed to integrate the GNU Portable Library Tool (libtool) and the GNU Libtool Dynamic Module Loader (ltdl) into a package built using the GNU Autotools (including GNU Autoconf and GNU Automake). This package includes a modification from the original GNU Libtool to allow support for multi-architecture systems, such as the AMD64 Opteron and the Intel 64-bit Xeon.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

#### libuser-0.54.7-2.el5.5 - libuser-0.54.7-2.1.el5\_4.1

- Group: System Environment/Base

- Summary: A user and group account administration library.
- Description: The libuser library implements a standardized interface for manipulating and administering user and group accounts. The library uses pluggable back-ends to interface to its data sources. Sample applications modeled after those included with the shadow password suite are included.
- Added Dependencies:
  - autoconf
  - automake
  - gettext-devel
  - gtk-doc
  - libtool
  - nscd
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libvirt-0.6.3-20.el5 - libvirt-0.6.3-33.el5

- Group: Development/Libraries
- Summary: Library providing a simple API virtualization
- Description: Libvirt is a C toolkit to interact with the virtualization capabilities of recent versions of Linux (and other OSes).
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

libvirt-cim-0.5.5-2.el5 - libvirt-cim-0.5.8-3.el5

- Group: Development/Libraries
- Summary: A CIM provider for libvirt
- Description: Libvirt-cim is a CMPI CIM provider that implements the DMTF SVPC virtualization model. The goal is to support most of the features exported by libvirt itself, enabling management of multiple platforms with a single provider.
- No added dependencies
- Removed Dependencies:
  - xen-devel
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libvorbis-1.1.2-3.el5\_3.3 - libvorbis-1.1.2-3.el5\_4.4

- Group: System Environment/Libraries
- Summary: The Vorbis General Audio Compression Codec.
- Description: Ogg Vorbis is a fully open, non-proprietary, patent-and royalty-free, general-purpose compressed audio format for audio and music at fixed and variable bitrates from 16 to 128 kbps/channel. The libvorbis package contains runtime libraries for use in programs that support Ogg Vorbis.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

## Appendix A. Package Manifest

---

linuxwacom-0.7.8.3-6.el5 - linuxwacom-0.7.8.3-8.el5

- Group: User Interface/X Hardware Support
- Summary: Wacom Drivers from Linux Wacom Project
- Description: The Linux Wacom Project manages the drivers, libraries, and documentation for configuring and running Wacom tablets under the Linux operating system. It contains diagnostic applications as well as X.org XInput drivers.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

lm\_sensors-2.10.7-4.el5 - lm\_sensors-2.10.7-9.el5

- Group: Applications/System
- Summary: Hardware monitoring tools.
- Description: The lm\_sensors package includes a collection of modules for general SMBus access and hardware monitoring. NOTE: this requires special support which is not in standard 2.2-vintage kernels.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

log4cpp-1.0-4.el5 - log4cpp-1.0-9.el5

- Group: Development/Libraries
- Summary: C++ logging library

- Description: A library of C++ classes for flexible logging to files, syslog, IDSA and other destinations. It is modeled after the Log for Java library (<http://www.log4j.org>), staying as close to their API as is reasonable.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

#### logwatch-7.3-6.el5 - logwatch-7.3-8.el5

- Group: Applications/System
- Summary: A log file analysis program
- Description: Logwatch is a customizable, pluggable log-monitoring system. It will go through your logs for a given period of time and make a report in the areas that you wish with the detail that you wish. Easy to use - works right out of the package on many systems.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

#### lvm2-2.02.46-8.el5 - lvm2-2.02.56-8.el5

- Group: System Environment/Base
- Summary: Userland logical volume management tools
- Description: LVM2 includes all of the support for handling read/write operations on physical volumes (hard disks, RAID-Systems, magneto optical, etc., multiple devices (MD), see `mdadd(8)` or even loop devices, see `losetup(8)`), creating volume groups (kind of virtual disks) from one or more physical volumes and creating one or more logical volumes (kind of logical partitions) in volume groups.

## Appendix A. Package Manifest

---

- Added Dependencies:
  - device-mapper >= 1.02.39-1
- Removed Dependencies:
  - device-mapper >= 1.02.32-1
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

lvm2-cluster-2.02.46-8.el5 - lvm2-cluster-2.02.56-7.el5

- Group: System Environment/Base
- Summary: Cluster extensions for userland logical volume management tools
- Description: Extensions to LVM2 to support clusters.
- Added Dependencies:
  - device-mapper >= 1.02.39-1
- Removed Dependencies:
  - device-mapper >= 1.02.32-1
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

man-pages-2.39-12.el5 - man-pages-2.39-15.el5

- Group: Documentation
- Summary: Man (manual) pages from the Linux Documentation Project.
- Description: A large collection of man pages (documentation) from the Linux Documentation Project (LDP).
- No added dependencies

- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

man-pages-ja-20060815-11.el5 - man-pages-ja-20060815-13.el5

- Group: Documentation
- Summary: Japanese man (manual) pages from the Japanese Manual Project
- Description: Japanese Manual pages, translated by JM-Project (Japanese Manual Project).
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mcelog-0.9pre-1.27.el5 - mcelog-0.9pre-1.29.el5

- Group: System Environment/Base
- Summary: Tool to translate x86-64 CPU Machine Check Exception data.
- Description: mcelog is a daemon that collects and decodes Machine Check Exception data on x86-64 machines.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts



## Appendix A. Package Manifest

---

- No added obsoletes
- No removed obsoletes

mdadm-2.6.9-2.el5 - mdadm-2.6.9-3.el5

- Group: System Environment/Base
- Summary: mdadm controls Linux md devices (software RAID arrays)
- Description: mdadm is used to create, manage, and monitor Linux MD (software RAID) devices. As such, it provides similar functionality to the raidtools package. However, mdadm is a single program, and it can perform almost all functions without a configuration file, though a configuration file can be used to help with some common tasks.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mesa-6.5.1-7.7.el5 - mesa-6.5.1-7.8.el5

- Group: System Environment/Libraries
- Summary: Mesa graphics libraries
- Description: Mesa
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

metacity-2.16.0-12.el5 - metacity-2.16.0-15.el5

- Group: User Interface/Desktops
- Summary: Metacity window manager

- Description: Metacity is a simple window manager that integrates nicely with GNOME 2.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

microcode\_ctl-1.17-1.48.el5 - microcode\_ctl-1.17-1.50.el5

- Group: System Environment/Base
- Summary: Tool to update x86/x86-64 CPU microcode.
- Description: microcode\_ctl - updates the microcode on Intel x86/x86-64 CPU's
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mkinitrd-5.1.19.6-54 - mkinitrd-5.1.19.6-61

- Group: System Environment/Base
- Summary: Creates an initial ramdisk image for preloading modules.
- Description: Mkinitrd creates filesystem images for use as initial ramdisk (initrd) images. These ramdisk images are often used to preload the block device modules (SCSI or RAID) needed to access the root filesystem. In other words, generic kernels can be built without drivers for any SCSI adapters which load the SCSI driver as a module. Since the kernel needs to read those modules, but in this case it isn't able to address the SCSI adapter, an initial ramdisk is used. The initial ramdisk is loaded by the operating system loader (normally LILO) and is available to the kernel as soon as the ramdisk is loaded. The ramdisk image loads the proper SCSI adapter and allows the kernel to mount the root filesystem. The mkinitrd program creates such a ramdisk using information found in the /etc/modules.conf file.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

module-init-tools-3.3-0.pre3.1.54.el5 - module-init-tools-3.3-0.pre3.1.60.el5

- Group: System Environment/Kernel
- Summary: Kernel module management utilities.
- Description: The modutils package includes various programs needed for automatic loading and unloading of modules under 2.6 and later kernels, as well as other module management programs. Device drivers and filesystems are two examples of loaded and unloaded modules.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mpitests-3.1-3.el5 - mpitests-3.2-1.el5

- Group: Applications
- Summary: MPI Benchmarks and tests
- Description: Set of popular MPI benchmarks: IMB-2.3 Presta-1.4.0 OSU benchmarks ver 2.2
- Added Dependencies:
  - mvapich >= 1.2.0
  - mvapich2 >= 1.4
  - openmpi >= 1.4
- Removed Dependencies:

- mvapich >= 1.1.0-0.3355.2
- mvapich2 >= 1.2-0.p1.3
- openmpi >= 1.3.2-2
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mtx-1.2.18-8.2.2 - mtx-1.2.18-9

- Group: Applications/System
- Summary: A SCSI media changer control program.
- Description: The MTX program controls the robotic mechanism in autoloaders and tape libraries such as the HP SureStore DAT 40x6, Exabyte EZ-17, and Exabyte 220. This program is also reported to work with a variety of other tape libraries and autochangers from ADIC, Tandberg/Overland, Breece Hill, HP, and Seagate. If you have a backup tape device capable of handling more than one tape at a time, you should install MTX.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mvapich-1.1.0-0.3355.2.el5 - mvapich-1.2.0-0.3562.1.el5

- Group: Development/Libraries
- Summary: MPI implementation over Infiniband RDMA-enabled interconnect
- Description: This is high performance and scalable MPI-1 implementation over Infiniband and RDMA-enabled interconnects. This implementation is based on MPICH and MVICH. MVAPICH is pronounced as `em-vah-pich".
- No added dependencies

- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mvapich2-1.2-0.p1.3.el5 - mvapich2-1.4-1.el5

- Group: Development/Libraries
- Summary: OSU MVAPICH2 MPI package
- Description: This is an MPI-2 implementation which includes all MPI-1 features. It is based on MPICH2 and MVICH.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mysql-5.0.77-3.el5 - mysql-5.0.77-4.el5\_4.2

- Group: Applications/Databases
- Summary: MySQL client programs and shared libraries
- Description: MySQL is a multi-user, multi-threaded SQL database server. MySQL is a client/server implementation consisting of a server daemon (mysqld) and many different client programs and libraries. The base package contains the MySQL client programs, the client shared libraries, and generic MySQL files.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

nautilus-open-terminal-0.6-6.el5 - nautilus-open-terminal-0.6-7.el5

- Group: User Interface/Desktops
- Summary: Nautilus extension for an open terminal shortcut
- Description: The nautilus-open-terminal extension provides a right-click "Open Terminal" option for nautilus users who prefer that option.
- Added Dependencies:
  - intltool
  - nautilus-devel >= 2.5.4
- Removed Dependencies:
  - nautilus >= 2.5.4
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

neon-0.25.5-10.el5 - neon-0.25.5-10.el5\_4.1

- Group: Applications/Publishing
- Summary: An HTTP and WebDAV client library
- Description: neon is an HTTP and WebDAV client library, with a C interface; providing a high-level interface to HTTP and WebDAV methods along with a low-level interface for HTTP request handling. neon supports persistent connections, proxy servers, basic, digest and Kerberos authentication, and has complete SSL support.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

## Appendix A. Package Manifest

---

- No added obsoletes
- No removed obsoletes

net-snmp-5.3.2.2-7.el5 - net-snmp-5.3.2.2-9.el5

- Group: System Environment/Daemons
- Summary: A collection of SNMP protocol tools and libraries.
- Description: SNMP (Simple Network Management Protocol) is a protocol used for network management. The NET-SNMP project includes various SNMP tools: an extensible agent, an SNMP library, tools for requesting or setting information from SNMP agents, tools for generating and handling SNMP traps, a version of the netstat command which uses SNMP, and a Tk/Perl mib browser. This package contains the snmpd and snmptrapd daemons, documentation, etc. You will probably also want to install the net-snmp-utils package, which contains NET-SNMP utilities. Building option: --without tcp\_wrappers : disable tcp\_wrappers support
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

net-tools-1.60-78.el5 - net-tools-1.60-81.el5

- Group: System Environment/Base
- Summary: Basic networking tools.
- Description: The net-tools package contains basic networking tools, including ifconfig, netstat, route, and others.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

newt-0.52.2-12.el5 - newt-0.52.2-15.el5

- Group: System Environment/Libraries
- Summary: A development library for text mode user interfaces.
- Description: Newt is a programming library for color text mode, widget based user interfaces. Newt can be used to add stacked windows, entry widgets, checkboxes, radio buttons, labels, plain text fields, scrollbars, etc., to text mode user interfaces. This package also contains the shared library needed by programs built with newt, as well as a `/usr/bin/dialog` replacement called `whiptail`. Newt is based on the slang library.
- Added Dependencies:
  - docbook-utils
  - lynx
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

nfs-utils-1.0.9-42.el5 - nfs-utils-1.0.9-44.el5

- Group: System Environment/Daemons
- Summary: NFS utilities and supporting clients and daemons for the kernel NFS server.
- Description: The `nfs-utils` package provides a daemon for the kernel NFS server and related tools, which provides a much higher level of performance than the traditional Linux NFS server used by most users. This package also contains the `showmount` program. `Showmount` queries the mount daemon on a remote host for information about the NFS (Network File System) server on the remote host. For example, `showmount` can display the clients which are mounted on that host. This package also contains the `mount.nfs` and `umount.nfs` program.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes



## Appendix A. Package Manifest

---

- No removed obsoletes

nspluginwrapper-0.9.91.5-22.el5 - nspluginwrapper-1.3.0-8.el5

- Group: Networking/WWW
- Summary: A compatibility layer for Netscape 4 plugins
- Description: nspluginwrapper makes it possible to use Netscape 4 compatible plugins compiled for ppc into Mozilla for another architecture, e.g. x86\_64. This package consists in: \* npviewer: the plugin viewer \* npwrapper.so: the browser-side plugin \* nspluginplayer: stand-alone NPAPI plugin player \* mozilla-plugin-config: a tool to manage plugins installation and update
- Added Dependencies:
  - curl-devel
  - gecko-devel
  - libX11-devel
  - nspr-devel
  - pango-devel
- Removed Dependencies:
  - gecko-devel >= 1.9
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

nspr-4.7.4-1.el5\_3.1 - nspr-4.7.6-1.el5\_4

- Group: System Environment/Libraries
- Summary: Netscape Portable Runtime
- Description: NSPR provides platform independence for non-GUI operating system facilities. These facilities include threads, thread synchronization, normal file and network I/O, interval timing and calendar time, basic memory management (malloc and free) and shared library linking.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

#### nss\_ldap-253-21.el5 - nss\_ldap-253-25.el5

- Group: System Environment/Base
- Summary: NSS library and PAM module for LDAP.
- Description: This package includes two LDAP access clients: nss\_ldap and pam\_ldap. Nss\_ldap is a set of C library extensions that allow X.500 and LDAP directory servers to be used as a primary source of aliases, ethers, groups, hosts, networks, protocol, users, RPCs, services, and shadow passwords (instead of or in addition to using flat files or NIS). Pam\_ldap is a module for Linux-PAM that supports password changes, V2 clients, Netscape's SSL, ypldapd, Netscape Directory Server password policies, access authorization, and crypted hashes.
- Added Dependencies:
  - openldap-devel >= 2.3.43-7
- Removed Dependencies:
  - openldap-devel >= 2.0.27
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

#### ntp-4.2.2p1-9.el5\_3.2 - ntp-4.2.2p1-9.el5\_4.1

- Group: System Environment/Daemons
- Summary: Synchronizes system time using the Network Time Protocol (NTP).
- Description: The Network Time Protocol (NTP) is used to synchronize a computer's time with another reference time source. The ntp package contains utilities and daemons that will synchronize your computer's time to Coordinated Universal Time (UTC) via the NTP protocol and NTP servers. The ntp package includes ntpdate (a program for retrieving the date and time from remote machines via a network) and ntpd (a daemon which continuously adjusts system time). Install the ntp package if you need tools for keeping your system's time synchronized via the NTP protocol.
- No added dependencies
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

numactl-0.9.8-8.el5 - numactl-0.9.8-11.el5

- Group: System Environment/Base
- Summary: library for tuning for Non Uniform Memory Access machines
- Description: Simple NUMA policy support. It consists of a numactl program to run other programs with a specific NUMA policy and a libnuma to do allocations with NUMA policy in applications.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openCryptoki-2.2.4-22.el5 - openCryptoki-2.2.4-22.el5\_4.2

- Group: Productivity/Security
- Summary: Implementation of Cryptoki v2.11 for IBM Crypto Hardware
- Description: The PKCS#11 Version 2.11 api implemented for the IBM Crypto cards. This package includes support for the IBM 4758 Cryptographic CoProcessor (with the PKCS#11 firmware loaded) and the IBM eServer Cryptographic Accelerator (FC 4960 on pSeries)
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

openais-0.80.6-8.el5 - openais-0.80.6-16.el5

- Group: System Environment/Base
- Summary: The openais Standards-Based Cluster Framework executive and APIs
- Description: This package contains the openais executive, openais service handlers, default configuration files and init script.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openib-1.4.1-3.el5 - openib-1.4.1-5.el5

- Group: System Environment/Base
- Summary: OpenIB Infiniband Driver Stack
- Description: User space initialization scripts for the kernel InfiniBand drivers
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openldap-2.3.43-3.el5 - openldap-2.3.43-12.el5

- Group: System Environment/Daemons
- Summary: The configuration files, libraries, and documentation for OpenLDAP.

- Description: OpenLDAP is an open source suite of LDAP (Lightweight Directory Access Protocol) applications and development tools. LDAP is a set of protocols for accessing directory services (usually phone book style information, but other information is possible) over the Internet, similar to the way DNS (Domain Name System) information is propagated over the Internet. The openldap package contains configuration files, libraries, and documentation for OpenLDAP.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

### openmotif-2.3.1-2.el5 - openmotif-2.3.1-2.el5\_4.1

- Group: System Environment/Libraries
- Summary: Open Motif runtime libraries and executables.
- Description: This is the Open Motif 2.3.1 runtime environment. It includes the Motif shared libraries, needed to run applications which are dynamically linked against Motif, and the Motif Window Manager "mwm".
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

### openmpi-1.3.2-2.el5 - openmpi-1.4-4.el5

- Group: Development/Libraries
- Summary: Open Message Passing Interface
- Description: Open MPI is an open source, freely available implementation of both the MPI-1 and MPI-2 standards, combining technologies and resources from several other projects (FT-MPI, LA-MPI, LAM/MPI, and PACX-MPI) in order to build the best MPI library available. A completely

new MPI-2 compliant implementation, Open MPI offers advantages for system and software vendors, application developers, and computer science researchers. For more information, see <http://www.open-mpi.org/> .

- Added Dependencies:
  - libibcm-devel
  - libibverbs-devel >= 1.1.3
  - librdmacm-devel
- Removed Dependencies:
  - compat-dapl-devel >= 2.0.19-2
  - libibverbs-devel >= 1.1.2-4
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openoffice.org-2.3.0-6.11.el5 - openoffice.org-3.1.1-19.5.el5

- Group: Applications/Productivity
- Summary: OpenOffice.org comprehensive office suite.
- Description: OpenOffice.org is an Open Source, community-developed, multi-platform office productivity suite. It includes the key desktop applications, such as a word processor, spreadsheet, presentation manager, formula editor and drawing program, with a user interface and feature set similar to other office suites. Sophisticated and flexible, OpenOffice.org also works transparently with a variety of file formats, including Microsoft Office. Usage: Simply type "ooffice" to run OpenOffice.org or select the requested component (Writer, Calc, Impress, etc.) from your desktop menu. On first start a few files will be installed in the user's home, if necessary.
- Added Dependencies:
  - bc
  - gperf
  - java-devel-gcj
  - lucene
- Removed Dependencies:

- java-devel = 1.4.2
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

opensm-3.2.6-2.el5 - opensm-3.3.3-1.el5

- Group: System Environment/Daemons
- Summary: OpenIB InfiniBand Subnet Manager and management utilities
- Description: OpenSM is the OpenIB project's Subnet Manager for Infiniband networks. The subnet manager is run as a system daemon on one of the machines in the infiniband fabric to manage the fabric's routing state. This package also contains various tools for diagnosing and testing Infiniband networks that can be used from any machine and do not need to be run on a machine running the opensm daemon.
- Added Dependencies:
  - byacc
  - libibmad-devel = 1.3.3
- Removed Dependencies:
  - libibmad-devel >= 1.2.3
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openssh-4.3p2-36.el5 - openssh-4.3p2-41.el5

- Group: Applications/Internet
- Summary: The OpenSSH implementation of SSH protocol versions 1 and 2
- Description: SSH (Secure SHell) is a program for logging into and executing commands on a remote machine. SSH is intended to replace rlogin and rsh, and to provide secure encrypted communications between two untrusted hosts over an insecure network. X11 connections and arbitrary TCP/IP ports can also be forwarded over the secure channel. OpenSSH is OpenBSD's

version of the last free version of SSH, bringing it up to date in terms of security and features, as well as removing all patented algorithms to separate libraries. This package includes the core files necessary for both the OpenSSH client and server. To make this package useful, you should also install openssh-clients, openssh-server, or both.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openssl-0.9.8e-12.el5 - openssl-0.9.8e-12.el5\_4.6

- Group: System Environment/Libraries
- Summary: The OpenSSL toolkit
- Description: The OpenSSL toolkit provides support for secure communications between machines. OpenSSL includes a certificate management tool and shared libraries which provide various cryptographic algorithms and protocols.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openswan-2.6.21-5.el5 - openswan-2.6.21-5.el5\_4.2

- Group: System Environment/Daemons
- Summary: Openswan IPSEC implementation
- Description: Openswan is a free implementation of IPsec & IKE for Linux. IPsec is the Internet Protocol Security and uses strong cryptography to provide both authentication and encryption services. These services allow you to build secure tunnels through untrusted networks. Everything passing through the untrusted net is encrypted by the ipsec gateway machine and decrypted by the gateway at the other end of the tunnel. The resulting tunnel is a virtual



private network or VPN. This package contains the daemons and userland tools for setting up Openswan. It supports the NETKEY/XFRM IPsec kernel stack that exists in the default Linux kernel. Openswan 2.6.x also supports IKEv2 (RFC4309)

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

oprofile-0.9.4-11.el5 - oprofile-0.9.4-15.el5

- Group: Development/System
- Summary: System wide profiler
- Description: OProfile is a profiling system for systems running Linux. The profiling runs transparently during the background, and profile data can be collected at any time. OProfile makes use of the hardware performance counters provided on Intel P6, and AMD Athlon family processors, and can use the RTC for profiling on other x86 processor types. See the HTML documentation for further details.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

pam-0.99.6.2-6.el5 - pam-0.99.6.2-6.el5\_4.1

- Group: System Environment/Base
- Summary: A security tool which provides authentication for applications
- Description: PAM (Pluggable Authentication Modules) is a system security tool that allows system administrators to set authentication policy without having to recompile programs that handle authentication.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

pam\_krb5-2.2.14-10 - pam\_krb5-2.2.14-15

- Group: System Environment/Base
- Summary: A Pluggable Authentication Module for Kerberos 5.
- Description: This is pam\_krb5, a pluggable authentication module that can be used with Linux-PAM and Kerberos 5. This module supports password checking, ticket creation, and optional TGT verification and conversion to Kerberos IV tickets. The included pam\_krb5afs module also gets AFS tokens if so configured.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

paps-0.6.6-18.el5 - paps-0.6.6-19.el5

- Group: Applications/Publishing
- Summary: Plain Text to PostScript converter
- Description: paps is a PostScript converter from plain text file using Pango.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

parted-1.8.1-23.el5 - parted-1.8.1-27.el5

- Group: Applications/System
- Summary: The GNU disk partition manipulation program
- Description: The GNU Parted program allows you to create, destroy, resize, move, and copy hard disk partitions. Parted can be used for creating space for new operating systems, reorganizing disk usage, and copying data to new hard disks.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

pax-3.4-1.2.2 - pax-3.4-2.el5

- Group: Applications/Archiving
- Summary: POSIX File System Archiver
- Description: 'pax' is the POSIX standard archive tool. It supports the two most common forms of standard Unix archive (backup) files - CPIO and TAR.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

pciutils-2.2.3-7.el5 - pciutils-2.2.3-8.el5

- Group: Applications/System
- Summary: PCI bus related utilities.
- Description: The pciutils package contains various utilities for inspecting and setting devices connected to the PCI bus. The utilities provided require kernel version 2.1.82 or newer (which support the /proc/bus/pci interface).
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

pcsc-lite-1.4.4-0.1.el5 - pcsc-lite-1.4.4-1.el5

- Group: System Environment/Daemons
- Summary: PC/SC Lite smart card framework and applications
- Description: The purpose of PC/SC Lite is to provide a Windows(R) SCard interface in a very small form factor for communicating to smartcards and readers. PC/SC Lite uses the same winscard API as used under Windows(R). This package includes the PC/SC Lite daemon, a resource manager that coordinates communications with smart card readers and smart cards that are connected to the system, as well as other command line tools.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

perftest-1.2-14.el5 - perftest-1.2.3-1.el5

- Group: Productivity/Networking/Diagnostic
- Summary: IB Performance tests

## Appendix A. Package Manifest

---

- Description: gen2 uverbs microbenchmarks
- Added Dependencies:
  - libibverbs-devel >= 1.1.3
  - librdmacm-devel >= 1.0.10
- Removed Dependencies:
  - libibverbs-devel >= 1.1.2-4
  - librdmacm-devel >= 1.0.8-5
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

perl-Sys-Virt-0.2.0-4.el5 - perl-Sys-Virt-0.2.0-6.el5

- Group: Development/Libraries
- Summary: Perl bindings for the libvirt library
- Description: The Sys::Virt module provides a Perl XS binding to the libvirt virtual machine management APIs. This allows machines running within arbitrary virtualization containers to be managed with a consistent API.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

perl-XML-LibXML-1.58-5 - perl-XML-LibXML-1.58-6

- Group: Development/Libraries
- Summary: XML-LibXML Perl module
- Description: XML-LibXML Perl module.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

perl-XML-SAX-0.14-5 - perl-XML-SAX-0.14-8

- Group: Development/Libraries
- Summary: XML-SAX Perl module
- Description: XML-SAX Perl module.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

pexpect-2.3-1.el5 - pexpect-2.3-3.el5

- Group: Development/Languages
- Summary: Pure Python Expect-like module
- Description: Pexpect is a pure Python module for spawning child applications; controlling them; and responding to expected patterns in their output. Pexpect works like Don Libes' Expect. Pexpect allows your script to spawn a child application and control it as if a human were typing commands. Pexpect can be used for automating interactive applications such as ssh, ftp, passwd, telnet, etc. It can be used to automate setup scripts for duplicating software package installations on different servers. And it can be used for automated software testing. Pexpect is in the spirit of Don Libes' Expect, but Pexpect is pure Python. Unlike other Expect-like modules for Python, Pexpect does not require TCL or Expect nor does it require C extensions to be compiled. It should work on any platform that supports the standard Python pty module.
- No added dependencies

- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

php-5.1.6-23.2.el5\_3 - php-5.1.6-27.el5

- Group: Development/Languages
- Summary: The PHP HTML-embedded scripting language. (PHP: Hypertext Preprocessor)
- Description: PHP is an HTML-embedded scripting language. PHP attempts to make it easy for developers to write dynamically generated webpages. PHP also offers built-in database integration for several commercial and non-commercial database management systems, so writing a database-enabled webpage with PHP is fairly simple. The most common use of PHP coding is probably as a replacement for CGI scripts. The php package contains the module which adds support for the PHP language to Apache HTTP Server.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

pidgin-2.5.9-1.el5 - pidgin-2.6.6-1.el5

- Group: Applications/Internet
- Summary: A Gtk+ based multiprotocol instant messaging client
- Description: Pidgin allows you to talk to anyone using a variety of messaging protocols including AIM, MSN, Yahoo!, Jabber, Bonjour, Gadu-Gadu, ICQ, IRC, Novell Groupwise, QQ, Lotus Sametime, SILC, Simple and Zephyr. These protocols are implemented using a modular, easy to use design. To use a protocol, just add an account using the account editor. Pidgin supports many common features of other clients, as well as many unique features, such as perl scripting, TCL scripting and C plugins. Pidgin is not affiliated with or endorsed by America Online, Inc., Microsoft Corporation, Yahoo! Inc., or ICQ Inc.
- No added dependencies

- Removed Dependencies:

- aspell-devel
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

piranha-0.8.4-13.el5 - piranha-0.8.4-16.el5

- Group: System Environment/Base
- Summary: Cluster administration tools
- Description: Various tools to administer and configure the Linux Virtual Server as well as heartbeating and failover components. The LVS is a dynamically adjusted kernel routing mechanism that provides load balancing primarily for web and ftp servers though other services are supported.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

pirut-1.3.28-13.el5 - pirut-1.3.28-17.el5

- Group: Applications/System
- Summary: Package Installation, Removal and Update Tools
- Description: pirut (pronounced "pirate") provides a set of graphical tools for managing software.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides



- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

policycoreutils-1.33.12-14.6.el5 - policycoreutils-1.33.12-14.8.el5

- Group: System Environment/Base
- Summary: SELinux policy core utilities.
- Description: Security-enhanced Linux is a feature of the Linux® kernel and a number of utilities with enhanced security functionality designed to add mandatory access controls to Linux. The Security-enhanced Linux kernel contains new architectural components originally developed to improve the security of the Flask operating system. These architectural components provide general support for the enforcement of many kinds of mandatory access control policies, including those based on the concepts of Type Enforcement®, Role-based Access Control, and Multi-level Security. policycoreutils contains the policy core utilities that are required for basic operation of a SELinux system. These utilities include load\_policy to load policies, setfiles to label filesystems, newrole to switch roles, and run\_init to run /etc/init.d scripts in the proper context.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

poppler-0.5.4-4.4.el5\_3.9 - poppler-0.5.4-4.4.el5\_4.11

- Group: Development/Libraries
- Summary: PDF rendering library
- Description: Poppler, a PDF rendering library, it's a fork of the xpdf PDF viewer developed by Derek Noonburg of Glyph and Cog, LLC.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

postgresql-8.1.11-1.el5\_1.1 - postgresql-8.1.18-2.el5\_4.1

- Group: Applications/Databases
- Summary: PostgreSQL client programs and libraries.
- Description: PostgreSQL is an advanced Object-Relational database management system (DBMS) that supports almost all SQL constructs (including transactions, subselects and user-defined types and functions). The postgresql package includes the client programs and libraries that you'll need to access a PostgreSQL DBMS server. These PostgreSQL client programs are programs that directly manipulate the internal structure of PostgreSQL databases on a PostgreSQL server. These client programs can be located on the same machine with the PostgreSQL server, or may be on a remote machine which accesses a PostgreSQL server over a network connection. This package contains the docs in HTML for the whole package, as well as command-line utilities for managing PostgreSQL databases on a PostgreSQL server. If you want to manipulate a PostgreSQL database on a remote PostgreSQL server, you need this package. You also need to install this package if you're installing the postgresql-server package.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ppc64-utils-0.11-12.el5 - ppc64-utils-0.11-14.el5

- Group: System Environment/Base
- Summary: Linux/PPC64 specific utilities
- Description: A collection of utilities for Linux on PPC64 platforms.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

procps-3.2.7-11.1.el5 - procps-3.2.7-16.el5

- Group: Applications/System
- Summary: System and process monitoring utilities.
- Description: The procps package contains a set of system utilities that provide system information. Procps includes ps, free, skill, pkill, pgrep, snice, tload, top, uptime, vmstat, w, watch and pwdx. The ps command displays a snapshot of running processes. The top command provides a repetitive update of the statuses of running processes. The free command displays the amounts of free and used memory on your system. The skill command sends a terminate command (or another specified signal) to a specified set of processes. The snice command is used to change the scheduling priority of specified processes. The tload command prints a graph of the current system load average to a specified tty. The uptime command displays the current time, how long the system has been running, how many users are logged on, and system load averages for the past one, five, and fifteen minutes. The w command displays a list of the users who are currently logged on and what they are running. The watch program watches a running program. The vmstat command displays virtual memory statistics about processes, memory, paging, block I/O, traps, and CPU activity. The pwdx command reports the current working directory of a process or processes.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

pykickstart-0.43.5-1.el5 - pykickstart-0.43.8-1.el5

- Group: System Environment/Libraries
- Summary: A python library for manipulating kickstart files
- Description: The pykickstart package is a python library for manipulating kickstart files.
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

python-virtinst-0.400.3-5.el5 - python-virtinst-0.400.3-9.el5

- Group: Development/Libraries
- Summary: Python modules and utilities for installing virtual machines
- Description: virtinst is a module that helps build and install libvirt based virtual machines. Currently supports KVM, QEmu and Xen virtual machines. Package includes several command line utilities, including virt-install (build and install new VMs) and virt-clone (clone an existing virtual machine).
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

qlvnictools-0.0.1-11.el5 - qlvnictools-0.0.1-12.el5

- Group: System Environment/Base
- Summary: VNIC ULP service
- Description: VNIC ULP service
- Added Dependencies:
  - libibverbs-devel
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

## Appendix A. Package Manifest

---

- No added obsoletes
- No removed obsoletes

qperf-0.4.4-3.el5 - qperf-0.4.6-1.el5

- Group: Networking/Diagnostic
- Summary: Measure socket and RDMA performance
- Description: Measure socket and RDMA performance.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

qspice-0.3.0-39.el5 - qspice-0.3.0-54.el5

- Group: User Interface/Desktops
- Summary: An implementation of the Simple Protocol for Independent Computing Environments
- Description: The Simple Protocol for Independent Computing Environments (SPICE) is a remote display system built for virtual environments which allows you to view a computing 'desktop' environment not only on the machine where it is running, but from anywhere on the Internet and from a wide variety of machine architectures.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rds-tools-1.4-2.el5 - rds-tools-1.5-1.el5

- Group: Applications/System
- Summary: RDS support tools

- Description: Various tools for support of the RDS (Reliable Datagram Socket) API. RDS is specific to InfiniBand and iWARP networks and does not work on non-RDMA hardware.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

#### readahead-1.3-7.el5 - readahead-1.3-8.el5

- Group: System Environment/Base
- Summary: Read a preset list of files into memory.
- Description: readahead reads the contents of a list of files into memory, which causes them to be read from cache when they are actually needed. Its goal is to speed up the boot process.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

#### redhat-artwork-5.0.9-1.el5 - redhat-artwork-5.0.9-2.el5

- Group: User Interface/Desktops
- Summary: Artwork for Red Hat default look-and-feel
- Description: redhat-artwork contains the themes and icons that make up the Red Hat default look and feel.
- No added dependencies
- No removed dependencies
- No added provides

## Appendix A. Package Manifest

---

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

redhat-release-5Client-5.4.0.3 - redhat-release-5Client-5.5.0.2

- Group: System Environment/Base
- Summary: Red Hat Enterprise Linux release file
- Description: Red Hat Enterprise Linux release files
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

redhat-release-notes-5Client-29 - redhat-release-notes-5Client-31

- Group: System Environment/Base
- Summary: Red Hat Enterprise Linux release notes files
- Description: Red Hat Enterprise Linux release notes files.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

redhat-release-5Server-5.4.0.3 - redhat-release-5Server-5.5.0.2

- Group: System Environment/Base
- Summary: Red Hat Enterprise Linux release file
- Description: Red Hat Enterprise Linux release files
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

redhat-release-notes-5Server-29 - redhat-release-notes-5Server-31

- Group: System Environment/Base
- Summary: Red Hat Enterprise Linux release notes files
- Description: Red Hat Enterprise Linux release notes files.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rgmanager-2.0.52-1.el5 - rgmanager-2.0.52-6.el5

- Group: System Environment/Base
- Summary: Open Source HA Resource Group Failover for Red Hat Enterprise Linux
- Description: Red Hat Resource Group Manager provides high availability of critical server applications in the event of planned or unplanned system downtime.
- No added dependencies
- No removed dependencies



## Appendix A. Package Manifest

---

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rhnc-client-tools-0.4.20-9.el5 - rhnc-client-tools-0.4.20-33.el5

- Group: System Environment/Base
- Summary: Support programs and libraries for Red Hat Network
- Description: Red Hat Network Client Tools provides programs and libraries to allow your system to receive software updates from Red Hat Network.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rhnlb-2.2.7-2.el5 - rhnlb-2.5.22-3.el5

- Group: Development/Libraries
- Summary: Python libraries for the RHN project
- Description: rhnlb is a collection of python modules used by the Red Hat Network (<http://rhn.redhat.com>) software.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

rhnsd-4.7.0-4.el5 - rhnsd-4.7.0-5.el5

- Group: System Environment/Base
- Summary: Red Hat Network query daemon
- Description: The Red Hat Update Agent that automatically queries the Red Hat Network servers and determines which packages need to be updated on your machine, and runs any actions.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rhpxl-0.41.1-7.el5 - rhpxl-0.41.1-9.el5

- Group: System Environment/Libraries
- Summary: Python library for configuring and running X.
- Description: The rhpxl (pronounced 'rapunzel') package contains a Python library for configuring and running X.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rsyslog-2.0.6-1.el5 - rsyslog-3.22.1-3.el5

- Group: System Environment/Daemons
- Summary: Enhanced system logging and kernel message trapping daemons
- Description: Rsyslog is an enhanced multi-threaded syslogd supporting, among others, MySQL, syslog/tcp, RFC 3195, permitted sender lists, filtering on any message part, and fine grain

output format control. It is quite compatible to stock syslogd and can be used as a drop-in replacement. Its advanced features make it suitable for enterprise-class, encryption protected syslog relay chains while at the same time being very easy to setup for the novice user.

- Added Dependencies:
  - gnutls-devel
  - krb5-devel
  - postgresql-devel
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ruby-1.8.5-5.el5\_3.7 - ruby-1.8.5-5.el5\_4.8

- Group: Development/Languages
- Summary: An interpreter of object-oriented scripting language
- Description: Ruby is the interpreted scripting language for quick and easy object-oriented programming. It has many features to process text files and to do system management tasks (as in Perl). It is simple, straight-forward, and extensible.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

samba-3.0.33-3.14.el5 - samba-3.0.33-3.28.el5

- Group: System Environment/Daemons
- Summary: The Samba SMB server.

- Description: Samba is the suite of programs by which a lot of PC-related machines share files, printers, and other information (such as lists of available files and printers). The Windows NT, OS/2, and Linux operating systems support this natively, and add-on packages can enable the same thing for DOS, Windows, VMS, UNIX of all kinds, MVS, and more. This package provides an SMB server that can be used to provide network services to SMB (sometimes called "Lan Manager") clients. Samba uses NetBIOS over TCP/IP (NetBT) protocols and does NOT need the NetBEUI (Microsoft Raw NetBIOS frame) protocol.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sblim-1-35.el5 - sblim-1-40.el5

- Group: Applications/System
- Summary: Standards Based Linux Instrumentation for Manageability
- Description: SBLIM stands for Standards Based Linux Instrumentation for Manageability, and consists of a set of standards based Web Based Enterprise Management (WBEM) modules that use the Common Information Model (CIM) standard to gather and provide systems management information, events, and methods to local or networked consumers via an CIM object services broker using the CMPI (Common Manageability Programming Interface) standard. This package provides a set of core providers and development tools for systems management applications.
- Added Dependencies:
  - libhbaapi-devel
  - openssl-devel
  - pam-devel
  - sblim-cmpi-devel
  - zlib-devel
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts

## Appendix A. Package Manifest

---

- No removed conflicts
- No added obsoletes
- No removed obsoletes

screen-4.0.3-1.el5 - screen-4.0.3-1.el5\_4.1

- Group: Applications/System
- Summary: A screen manager that supports multiple logins on one terminal
- Description: The screen utility allows you to have multiple logins on just one terminal. Screen is useful for users who telnet into a machine or are connected via a dumb terminal, but want to use more than just one login. Install the screen package if you need a screen manager that can support multiple logins on one terminal.
- Added Dependencies:
  - libutempter-devel
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

scsi-target-utils-0.0-5.20080917snap.el5 - scsi-target-utils-0.0-6.20091205snap.el5\_4.1

- Group: System Environment/Daemons
- Summary: The SCSI target daemon and utility programs
- Description: The SCSI target package contains the daemon and tools to setup a SCSI targets. Currently, software iSCSI targets are supported.
- No added dependencies
- Removed Dependencies:
  - openssl-devel
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

selinux-policy-2.4.6-255.el5 - selinux-policy-2.4.6-279.el5

- Group: System Environment/Base
- Summary: SELinux policy configuration
- Description: SELinux Reference Policy - modular.
- Added Dependencies:
  - checkpolicy >= 1.33.1-5
- Removed Dependencies:
  - checkpolicy >= 1.30.11-1
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sendmail-8.13.8-2.el5 - sendmail-8.13.8-8.el5

- Group: System Environment/Daemons
- Summary: A widely used Mail Transport Agent (MTA).
- Description: The Sendmail program is a very widely used Mail Transport Agent (MTA). MTAs send mail from one machine to another. Sendmail is not a client program, which you use to read your email. Sendmail is a behind-the-scenes program which actually moves your email over networks or the Internet to where you want it to go. If you ever need to reconfigure Sendmail, you will also need to have the sendmail.cf package installed. If you need documentation on Sendmail, you can install the sendmail-doc package.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

shadow-utils-4.0.17-14.el5 - shadow-utils-4.0.17-15.el5

- Group: System Environment/Base
- Summary: Utilities for managing accounts and shadow password files.
- Description: The shadow-utils package includes the necessary programs for converting UNIX password files to the shadow password format, plus programs for managing user and group accounts. The pwconv command converts passwords to the shadow password format. The pwunconv command unconverts shadow passwords and generates an npasswd file (a standard UNIX password file). The pwck command checks the integrity of password and shadow files. The lastlog command prints out the last login times for all users. The useradd, userdel, and usermod commands are used for managing user accounts. The groupadd, groupdel, and groupmod commands are used for managing group accounts.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sos-1.7-9.27.el5 - sos-1.7-9.49.el5

- Group: Development/Libraries
- Summary: A set of tools to gather troubleshooting information from a system
- Description: Sos is a set of tools that gathers information about system hardware and configuration. The information can then be used for diagnostic purposes and debugging. Sos is commonly used to help support technicians and developers.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

## squid-2.6.STABLE21-3.el5 - squid-2.6.STABLE21-6.el5

- Group: System Environment/Daemons
- Summary: The Squid proxy caching server.
- Description: Squid is a high-performance proxy caching server for Web clients, supporting FTP, gopher, and HTTP data objects. Unlike traditional caching software, Squid handles all requests in a single, non-blocking, I/O-driven process. Squid keeps meta data and especially hot objects cached in RAM, caches DNS lookups, supports non-blocking DNS lookups, and implements negative caching of failed requests. Squid consists of a main server program squid, a Domain Name System lookup program (dnsserver), a program for retrieving FTP data (ftpget), and some management and client tools.
- Added Dependencies:
  - krb5-devel
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

## squirrelmail-1.4.8-5.el5\_3.7 - squirrelmail-1.4.8-5.el5\_4.10

- Group: Applications/Internet
- Summary: SquirrelMail webmail client
- Description: SquirrelMail is a standards-based webmail package written in PHP4. It includes built-in pure PHP support for the IMAP and SMTP protocols, and all pages render in pure HTML 4.0 (with no Javascript) for maximum compatibility across browsers. It has very few requirements and is very easy to configure and install. SquirrelMail has all the functionality you would want from an email client, including strong MIME support, address books, and folder manipulation.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes



## Appendix A. Package Manifest

---

- No removed obsoletes

srptools-0.0.4-6.el5 - srptools-0.0.4-8.el5

- Group: System Environment/Base
- Summary: Tools for using the InfiniBand SRP protocol devices
- Description: In conjunction with the kernel ib\_srp driver, srptools allows you to discover and use SCSI devices via the SCSI RDMA Protocol over InfiniBand.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

star-1.5a75-2 - star-1.5a75-3

- Group: Applications/Archiving
- Summary: An archiving tool with ACL support
- Description: Star saves many files together into a single tape or disk archive, and can restore individual files from the archive. Star supports ACL.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

strace-4.5.18-5.el5 - strace-4.5.18-5.el5\_4.1

- Group: Development/Debuggers
- Summary: Tracks and displays system calls associated with a running process
- Description: The strace program intercepts and records the system calls called and received by a running process. Strace can print a record of each system call, its arguments and its return

value. Strace is useful for diagnosing problems and debugging, as well as for instructional purposes. Install strace if you need a tool to track the system calls made and received by a process.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sudo-1.6.9p17-5.el5 - sudo-1.7.2p1-5.el5

- Group: Applications/System
- Summary: Allows restricted root access for specified users.
- Description: Sudo (superuser do) allows a system administrator to give certain users (or groups of users) the ability to run some (or all) commands as root while logging all commands and arguments. Sudo operates on a per-command basis. It is not a replacement for the shell. Features include: the ability to restrict what commands a user may run on a per-host basis, copious logging of each command (providing a clear audit trail of who did what), a configurable timeout of the sudo command, and the ability to use the same configuration file (sudoers) on many different machines.
- Added Dependencies:
  - libselinux-devel
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sysklogd-1.4.1-44.el5 - sysklogd-1.4.1-46.el5

- Group: System Environment/Daemons
- Summary: System logging and kernel message trapping daemons.

- Description: The syslogd package contains two system utilities (syslogd and klogd) which provide support for system logging. Syslogd and klogd run as daemons (background processes) and log system messages to different places, like sendmail logs, security logs, error logs, etc.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

system-config-cluster-1.0.57-1.5 - system-config-cluster-1.0.57-3

- Group: Applications/System
- Summary: system-config-cluster is a utility which allows you to manage cluster configuration in a graphical setting.
- Description: system-config-cluster is a utility which allows you to manage cluster configuration in a graphical setting.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

system-config-lvm-1.1.5-1.0.el5 - system-config-lvm-1.1.5-4.el5

- Group: Applications/System
- Summary: A utility for graphically configuring Logical Volumes
- Description: system-config-lvm is a utility for graphically configuring Logical Volumes
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

system-config-securitylevel-1.6.29.1-2.1.el5 - system-config-securitylevel-1.6.29.1-5.el5

- Group: System Environment/Base
- Summary: A graphical interface for modifying the system security level
- Description: system-config-securitylevel is a graphical user interface for setting basic firewall rules.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

system-config-services-0.9.4-1.el5 - system-config-services-0.9.4-5.el5

- Group: Applications/System
- Summary: system-config-services is an initscript and xinetd configuration utility
- Description: system-config-services is a utility which allows you to configure which services should be enabled on your machine.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

systemtap-0.9.7-5.el5 - systemtap-1.1-3.el5

- Group: Development/System
- Summary: Instrumentation System
- Description: SystemTap is an instrumentation system for systems running Linux 2.6. Developers can write instrumentation to collect data on the operation of the system.
- Added Dependencies:
  - boost-devel
  - nss-tools
  - pkgconfig
- Removed Dependencies:
  - crash-devel
  - zlib-devel
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

tar-1.15.1-23.0.1.el5 - tar-1.15.1-30.el5

- Group: Applications/Archiving
- Summary: A GNU file archiving program
- Description: The GNU tar program saves many files together in one archive and can restore individual files (or all of the files) from that archive. Tar can also be used to add supplemental files to an archive and to update or list files in the archive. Tar includes multivolume support, automatic archive compression/decompression, the ability to perform remote archives, and the ability to perform incremental and full backups. If you want to use tar for remote backups, you also need to install the rmt package.
- Added Dependencies:
  - gawk
  - gettext
  - rsh
  - texinfo
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

#### taskjuggler-2.2.0-3 - taskjuggler-2.2.0-5.e15

- Group: Applications/Productivity
- Summary: Project management tool
- Description: TaskJuggler is a modern and powerful project management tool. Its new approach to project planning and tracking is far superior to the commonly used Gantt chart editing tools. It has already been successfully used in many projects and scales easily to projects with hundreds of resources and thousands of tasks. It covers the complete spectrum of project management tasks from the first idea to the completion of the project. It assists you during project scoping, resource assignment, cost and revenue planning, and risk and communication management.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

#### tcpdump-3.9.4-14.e15 - tcpdump-3.9.4-15.e15

- Group: Applications/Internet
- Summary: A network traffic monitoring tool.
- Description: Tcpdump is a command-line tool for monitoring network traffic. Tcpdump can capture and display the packet headers on a particular network interface or on all interfaces. Tcpdump can display all of the packet headers, or just the ones that match particular criteria. Install tcpdump if you need a program to monitor network traffic.
- No added dependencies
- No removed dependencies
- No added provides

## Appendix A. Package Manifest

---

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

tcsh-6.14-14.el5 - tcsh-6.14-17.el5

- Group: System Environment/Shells
- Summary: An enhanced version of csh, the C shell.
- Description: Tcsh is an enhanced but completely compatible version of csh, the C shell. Tcsh is a command language interpreter which can be used both as an interactive login shell and as a shell script command processor. Tcsh includes a command line editor, programmable word completion, spelling correction, a history mechanism, job control and a C language like syntax.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

thunderbird-2.0.0.22-2.el5\_3 - thunderbird-2.0.0.24-2.el5\_4

- Group: Applications/Internet
- Summary: Mozilla Thunderbird mail/newsgroup client
- Description: Mozilla Thunderbird is a standalone mail and newsgroup client.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

tog-pegasus-2.7.2-1.el5 - tog-pegasus-2.9.1-2.el5

- Group: Systems Management/Base
- Summary: OpenPegasus WBEM Services for Linux
- Description: OpenPegasus WBEM Services for Linux enables management solutions that deliver increased control of enterprise resources. WBEM is a platform and resource independent DMTF standard that defines a common information model and communication protocol for monitoring and controlling resources from diverse sources.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

tzdata-2009k-1.el5 - tzdata-2010e-1.el5

- Group: System Environment/Base
- Summary: Timezone data
- Description: This package contains data files with rules for various timezones around the world.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

util-linux-2.13-0.52.el5 - util-linux-2.13-0.52.el5\_4.1

- Group: System Environment/Base
- Summary: A collection of basic system utilities.



- Description: The util-linux package contains a large variety of low-level system utilities that are necessary for a Linux system to function. Among others, Util-linux contains the fdisk configuration tool and the login program.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

### valgrind-3.2.1-6.el5 - valgrind-3.5.0-1.el5

- Group: Development/Debuggers
- Summary: Tool for finding memory management bugs in programs
- Description: Valgrind is a tool to help you find memory-management problems in your programs. When a program is run under Valgrind's supervision, all reads and writes of memory are checked, and calls to malloc/new/free/delete are intercepted. As a result, Valgrind can detect a lot of problems that are otherwise very hard to find/diagnose.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

### vconfig-1.9-2.1 - vconfig-1.9-3

- Group: System Environment/Base
- Summary: Linux 802.1q VLAN configuration utility
- Description: The vconfig program configures and adjusts 802.1q VLAN parameters.
- No added dependencies
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

vino-2.13.5-7.el5 - vino-2.13.5-9.el5

- Group: User Interface/Desktops
- Summary: A remote desktop system for GNOME
- Description: Vino is a VNC server for GNOME. It allows remote users to connect to a running GNOME session using VNC.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

virt-manager-0.6.1-8.el5 - virt-manager-0.6.1-12.el5

- Group: Applications/Emulators
- Summary: Virtual Machine Manager
- Description: Virtual Machine Manager provides a graphical tool for administering virtual machines for KVM, Xen, and QEmu. Start, stop, add or remove virtual devices, connect to a graphical or serial console, and see resource usage statistics for existing VMs on local or remote machines. Uses libvirt as the backend management API.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

## Appendix A. Package Manifest

---

- No added obsoletes
- No removed obsoletes

vixie-cron-4.1-76.el5 - vixie-cron-4.1-77.el5\_4.1

- Group: System Environment/Base
- Summary: The Vixie cron daemon for executing specified programs at set times.
- Description: The vixie-cron package contains the Vixie version of cron. Cron is a standard UNIX daemon that runs specified programs at scheduled times. Vixie cron adds better security and more powerful configuration options to the standard version of cron.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

vsftpd-2.0.5-16.el5 - vsftpd-2.0.5-16.el5\_4.1

- Group: System Environment/Daemons
- Summary: vsftpd - Very Secure Ftp Daemon
- Description: vsftpd is a Very Secure FTP daemon. It was written completely from scratch.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

wdaemon-0.14-4 - wdaemon-0.14-5

- Group: User Interface/X Hardware Support
- Summary: Hotplug helper for Wacom X.org driver

- Description: Helper application which emulates persistent input devices for Wacom tablets so they can be plugged and unplugged while X.org server is running. This should go away as soon X.org properly supports hotplugging.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

#### wget-1.11.4-2.el5 - wget-1.11.4-2.el5\_4.1

- Group: Applications/Internet
- Summary: A utility for retrieving files using the HTTP or FTP protocols.
- Description: GNU Wget is a file retrieval utility which can use either the HTTP or FTP protocols. Wget features include the ability to work in the background while you are logged out, recursive retrieval of directories, file name wildcard matching, remote file timestamp storage and comparison, use of Rest with FTP servers and Range with HTTP servers to retrieve files over slow or unstable connections, support for Proxy servers, and configurability.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

#### wpa\_supplicant-0.5.10-8.el5 - wpa\_supplicant-0.5.10-9.el5

- Group: System Environment/Base
- Summary: WPA/WPA2/IEEE 802.1X Supplicant
- Description: wpa\_supplicant is a WPA Supplicant for Linux, BSD and Windows with support for WPA and WPA2 (IEEE 802.11i / RSN). Supplicant is the IEEE 802.1X/WPA component that is used in the client stations. It implements key negotiation with a WPA Authenticator and it controls the roaming and IEEE 802.11 authentication/association of the wlan driver.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xen-3.0.3-94.el5 - xen-3.0.3-105.el5

- Group: Development/Libraries
- Summary: Xen is a virtual machine monitor
- Description: This package contains the Xen tools and management daemons needed to run virtual machines on x86, x86\_64, and ia64 systems. Information on how to use Xen can be found at the Xen project pages. The Xen system also requires the Xen hypervisor and domain-0 kernel, which can be found in the kernel-xen\* package. Virtualization can be used to run multiple operating systems on one physical system, for purposes of hardware consolidation, hardware abstraction, or to test untrusted applications in a sandboxed environment.
- Added Dependencies:
  - bzip2-devel
  - e4fsprogs-devel
  - xz-devel
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xerces-j2-2.7.1-7jpp.2 - xerces-j2-2.7.1-7jpp.2.el5\_4.2

- Group: Text Processing/Markup/XML
- Summary: Java XML parser
- Description: Welcome to the future! Xerces2 is the next generation of high performance, fully compliant XML parsers in the Apache Xerces family. This new version of Xerces introduces

the Xerces Native Interface (XNI), a complete framework for building parser components and configurations that is extremely modular and easy to program. The Apache Xerces2 parser is the reference implementation of XNI but other parser components, configurations, and parsers can be written using the Xerces Native Interface. For complete design and implementation documents, refer to the XNI Manual. Xerces 2 is a fully conforming XML Schema processor. For more information, refer to the XML Schema page. Xerces 2 also provides a partial implementation of Document Object Model Level 3 Core, Load and Save and Abstract Schemas [deprecated] Working Drafts. For more information, refer to the DOM Level 3 Implementation page.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

#### xmlsec1-1.2.9-8.1 - xmlsec1-1.2.9-8.1.1

- Group: Development/Libraries
- Summary: Library providing support for "XML Signature" and "XML Encryption" standards
- Description: XML Security Library is a C library based on LibXML2 and OpenSSL. The library was created with a goal to support major XML security standards "XML Digital Signature" and "XML Encryption".
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

#### xorg-x11-drivers-7.1-4.1.el5 - xorg-x11-drivers-7.1-4.2.el5

- Group: User Interface/X Hardware Support
- Summary: X.Org X11 driver installation package

## Appendix A. Package Manifest

---

- Description: The purpose of this package is to require all of the individual X.Org driver rpms, to allow the OS installation software to install all drivers all at once, without having to track which individual drivers are present on each architecture. By installing this package, it forces all of the individual driver packages to be installed.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xorg-x11-drv-ast-0.81.0-3 - xorg-x11-drv-ast-0.89.9-1.e15

- Group: User Interface/X Hardware Support
- Summary: Xorg X11 ast video driver
- Description: X.Org X11 ast video driver.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xorg-x11-drv-evdev-1.0.0.5-3.e15 - xorg-x11-drv-evdev-1.0.0.5-5.e15

- Group: User Interface/X Hardware Support
- Summary: Xorg X11 evdev input driver
- Description: X.Org X11 evdev input driver.
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xorg-x11-drv-fbdev-0.3.0-2 - xorg-x11-drv-fbdev-0.3.0-3

- Group: User Interface/X Hardware Support
- Summary: Xorg X11 fbdev video driver
- Description: X.Org X11 fbdev video driver.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xorg-x11-drv-i810-1.6.5-9.25.el5 - xorg-x11-drv-i810-1.6.5-9.36.el5

- Group: User Interface/X Hardware Support
- Summary: Xorg X11 i810 video driver(s)
- Description: X.Org X11 i810 video driver.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes



## Appendix A. Package Manifest

---

xorg-x11-drv-mga-1.4.10-5.el5 - xorg-x11-drv-mga-1.4.10-7.el5

- Group: User Interface/X Hardware Support
- Summary: Xorg X11 mga video driver
- Description: X.Org X11 mga video driver.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xorg-x11-drv-nv-2.1.12-6.el5 - xorg-x11-drv-nv-2.1.15-3.el5

- Group: User Interface/X Hardware Support
- Summary: Xorg X11 nv video driver
- Description: X.Org X11 nv video driver.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xorg-x11-drv-qxl-0.0.4-1.1.el5 - xorg-x11-drv-qxl-0.0.12-1.2.el5

- Group: User Interface/X Hardware Support
- Summary: Xorg X11 qxl video driver
- Description: X.Org X11 qxl video driver.
- No added dependencies
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xorg-x11-drv-vesa-1.3.0-8.1.el5 - xorg-x11-drv-vesa-1.3.0-8.2.el5

- Group: User Interface/X Hardware Support
- Summary: Xorg X11 vesa video driver
- Description: X.Org X11 vesa video driver.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xorg-x11-server-1.1.1-48.67.el5 - xorg-x11-server-1.1.1-48.76.el5

- Group: User Interface/X
- Summary: X.Org X11 X server
- Description: X.Org X11 X server
- Added Dependencies:
  - mesa-source >= 6.5.1-7.8.el5
  - pam-devel
- Removed Dependencies:
  - mesa-source >= 6.5.1
- No added provides
- No removed provides
- No added conflicts

## Appendix A. Package Manifest

---

- No removed conflicts
- No added obsoletes
- No removed obsoletes

xorg-x11-xdm-1.0.5-6.el5 - xorg-x11-xdm-1.0.5-7.el5

- Group: User Interface/X
- Summary: X.Org X11 xdm - X Display Manager
- Description: X.Org X11 xdm - X Display Manager
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xterm-215-8.el5 - xterm-215-8.el5\_4.1

- Group: User Interface/X
- Summary: xterm terminal emulator for the X Window System
- Description: The xterm program is a terminal emulator for the X Window System. It provides DEC VT102 and Tektronix 4014 compatible terminals for programs that can't use the window system directly.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xulrunner-1.9.0.12-1.el5\_3 - xulrunner-1.9.0.18-1.el5\_4

- Group: Applications/Internet

- Summary: XUL Runtime for Gecko Applications
- Description: XULRunner provides the XUL Runtime environment for Gecko applications.
- Added Dependencies:
  - nspr-devel >= 4.7.6
- Removed Dependencies:
  - nspr-devel >= 4.7.0.99.2
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

#### yaboot-1.3.13-8.el5 - yaboot-1.3.13-10.el5

- Group: System Environment/Base
- Summary: Linux bootloader for Power Macintosh "New World" computers.
- Description: yaboot is a bootloader for PowerPC machines which works on New World ROM machines (Rev. A iMac and newer) and runs directly from Open Firmware, eliminating the need for Mac OS. yaboot can also bootload IBM pSeries machines.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

#### yp-tools-2.9-0.1 - yp-tools-2.9-1.el5

- Group: System Environment/Base
- Summary: NIS (or YP) client programs.
- Description: The Network Information Service (NIS) is a system which provides network information (login names, passwords, home directories, group information) to all of the machines on a network. NIS can enable users to login on any machine on the network, as long

as the machine has the NIS client programs running and the user's password is recorded in the NIS passwd database. NIS was formerly known as Sun Yellow Pages (YP). This package's NIS implementation is based on FreeBSD's YP and is a special port for glibc 2.x and libc versions 5.4.21 and later. This package only provides the NIS client programs. In order to use the clients, you'll need to already have an NIS server running on your network. An NIS server is provided in the ypserv package. Install the yp-tools package if you need NIS client programs for machines on your network. You will also need to install the ypbind package on every machine running NIS client programs. If you need an NIS server, you'll need to install the ypserv package on one machine on the network.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

yum-3.2.22-20.el5 - yum-3.2.22-26.el5

- Group: System Environment/Base
- Summary: RPM installer/updater
- Description: Yum is a utility that can check for and automatically download and install updated RPM packages. Dependencies are obtained and downloaded automatically prompting the user as necessary.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

yum-rhn-plugin-0.5.4-13.el5 - yum-rhn-plugin-0.5.4-15.el5

- Group: System Environment/Base
- Summary: RHN support for yum

- Description: This yum plugin provides support for yum to access a Red Hat Network server for software updates.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes



---

## Appendix B. Revision History

Revision 1.01 Thu Apr 22 2009

Ryan Lerch [r1erch@redhat.com](mailto:r1erch@redhat.com)

Added new Known Issue for Bug 575799

Revision 1.0 Wed Nov 26 2009

Ryan Lerch [r1erch@redhat.com](mailto:r1erch@redhat.com)

Initial Build of the 5.5 Technical Notes



