Red Hat Enterprise Linux 5

5.7 Technical Notes

Detailed notes on the changes implemented in Red Hat Enterprise Linux 5.7

Edition 7

Last Updated: 2017-11-14

Red Hat Enterprise Linux 5 5.7 Technical Notes

Detailed notes on the changes implemented in Red Hat Enterprise Linux 5.7

Edition 7

Legal Notice

Abstract

The Red Hat Enterprise Linux 5.7 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 5.6 and minor release Red Hat Enterprise Linux 5.7.

Table of Contents

PREFACE

The *Red Hat Enterprise Linux 5.7 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 5.6 and minor release Red Hat Enterprise Linux 5.7.

For system administrators and others planning Red Hat Enterprise Linux 5.7 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 5.7 Technical Notes* provide a single, organized source for change tracking and compliance testing.

For every user, the *Red Hat Enterprise Linux 5.7 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.

CHAPTER 1. PACKAGE UPDATES

1.1. ACROREAD

1.1.1. RHSA-2011:0301: Critical acroread security update

Updated acroread packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4 Extras and Red Hat Enterprise Linux 5 and 6 Supplementary.

The Red Hat Security Response Team has rated this update as having critical 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.

Adobe Reader allows users to view and print documents in Portable Document Format (PDF).

This update fixes multiple vulnerabilities in Adobe Reader. These vulnerabilities are detailed on the Adobe security page APSB11-03, listed in the References section.

A specially-crafted PDF file could cause Adobe Reader to crash or, potentially, execute arbitrary code as the user running Adobe Reader when opened. (CVE-2011-0562, CVE-2011-0563, CVE-2011-0565, CVE-2011-0566, CVE-2011-0567, CVE-2011-0585, CVE-2011-0586, CVE-2011-0589, CVE-2011-0590, CVE-2011-0591, CVE-2011-0592, CVE-2011-0593, CVE-2011-0594, CVE-2011-0595, CVE-2011-0596, CVE-2011-0598, CVE-2011-0599, CVE-2011-0600, CVE-2011-0602, CVE-2011-0603, CVE-2011-0606)

Multiple security flaws were found in Adobe reader. A specially-crafted PDF file could cause cross-site scripting (XSS) attacks against the user running Adobe Reader when opened. (CVE-2011-0587, CVE-2011-0604)

All Adobe Reader users should install these updated packages. They contain Adobe Reader version 9.4.2, which is not vulnerable to these issues. All running instances of Adobe Reader must be restarted for the update to take effect.

1.2. ANACONDA

1.2.1. RHBA-2011:0984: anaconda bug fix and enhancement update

Updated anaconda packages that fix multiple bugs and add multiple enhancements are now available for Red Hat Enterprise Linux 5.

The anaconda packages provide the installation program used by Red Hat Enterprise Linux to identify and configure the hardware, and to create the appropriate file systems for the system's architecture, as well as to to install the operating system software.

This update fixes the following bugs:

* Some packages could be lost when initiating a kickstart with selected virtualization software. Now, anaconda validates package repositories added via kickstart against the installation key if one is given. (BZ#452983)

* When installing all packages in a paravirtualized Xen guest, the wrong kernel was set as default. Now, anaconda sets kernel-xen as the default kernel for installations on Xen guests. (BZ#480031)

* When booting with a kernel boot command, anaconda could abort unexpectedly. Now, anaconda no longer aborts when booted with a kernel boot command-line that ends with a quote character. (BZ#500198)

* Drives to be moved up or down in the "Edit the Driver Order" dialog had to be re-selected each time they moved one position up or down. Now, anaconda no longer deselects selected items when moving them. (BZ#583837)

* When pressing the 'Back' button on the package confirmation screen, incorrect packages could be installed. Now, packages are installed as expected. (BZ#603177)

* The file systems ext3 and ext4 had incompatible mount options when created. Now, both ext3 and ext4 file systems have the same default mount options. (BZ#616184)

* anaconda incorrectly referred to installation DVDs as "CD". Now, this problem is resolved. (BZ#617262, BZ#641412)

* If a 0-byte storage device was present, anaconda aborted unexpectedly. Now, anaconda no longer aborts when a device of 0 bytes is present on the system. (BZ#636984)

* The iBFT code selected the wrong LAN interface for installation. Now, anaconda activates the correct network interface when there are multiple networks available and one of them has iBFT data. (BZ#643774)

* The hard drive installation method and layer2 VSWITCH caused non-functional networking on the IBM System z. Now, anaconda writes out the LAYER2 and PORTNO options into ifcfg files also on non-network install methods. (BZ#649301)

* It was not possible to go back to the Partition screen during VNC installation on the IBM System z. Now, anaconda allows the user to go back from the network screen to the partitioning screen. (BZ#654685)

* An unexpected SELinux context was set in the iptables configuration file. Now, anaconda sets the correct SELinux context. (BZ#658084)

* The kickstart files on USB drives were not found on the first attempt. Now, anaconda only asks to retry reading the kickstart file from a CD-ROM drive when necessary. Now, the drive probing handles situations better when the device shows up late. (BZ#658398)

* ETHTOOL_OPT in ifcfg-ethX was not quoted with the kickstart option --ethtool. Now, anaconda correctly quotes ETHTOOL_OPTS in ifcfg files. (BZ#674473)

* Now, anaconda enables IPv6 on the installed system unless this is explicitly disabled via kickstart. (BZ#677653)

This update also adds the following enhancements:

* It is now possible to disable ssh via Anaconda kickstart command such as "firewall --enabled --no-ssh". (BZ#485086)

* Busybox is now a part of the installation RAM Disk image to allow for easier debugging of installation issues. (BZ#500527)

* A new kernel boot command-line argument blacklist= is now recognized in Anaconda that lets the user blacklist troubling drivers. Such drivers are then not loaded by Anaconda. (BZ#569883)

* Now, the Anaconda installer contains and runs the Red Hat Subscription Manager and associated yum plugins. (BZ#670973)

All users are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

1.3. APR

1.3.1. RHSA-2011:0844: Low apr security update

Updated apr packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

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 Apache Portable Runtime (APR) is a portability library used by the Apache HTTP Server and other projects. It provides a free library of C data structures and routines.

The fix for CVE-2011-0419 (released via RHSA-2011:0507) introduced an infinite loop flaw in the apr_fnmatch() function when the APR_FNM_PATHNAME matching flag was used. A remote attacker could possibly use this flaw to cause a denial of service on an application using the apr_fnmatch() function. (CVE-2011-1928)

Note: This problem affected httpd configurations using the "Location" directive with wildcard URLs. The denial of service could have been triggered during normal operation; it did not specifically require a malicious HTTP request.

This update also addresses additional problems introduced by the rewrite of the apr_fnmatch() function, which was necessary to address the CVE-2011-0419 flaw.

All apr users should upgrade to these updated packages, which contain a backported patch to correct this issue. Applications using the apr library, such as httpd, must be restarted for this update to take effect.

1.3.2. RHSA-2011:0507: Moderate apr security update

Updated apr packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

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 Apache Portable Runtime (APR) is a portability library used by the Apache HTTP Server and other projects. It provides a free library of C data structures and routines.

It was discovered that the apr_fnmatch() function used an unconstrained recursion when processing patterns with the '*' wildcard. An attacker could use this flaw to cause an application using this function, which also accepted untrusted input as a pattern for matching (such as an httpd server using the mod_autoindex module), to exhaust all stack memory or use an excessive amount of CPU time when performing matching. (CVE-2011-0419)

Red Hat would like to thank Maksymilian Arciemowicz for reporting this issue.

All apr users should upgrade to these updated packages, which contain a backported patch to correct this issue. Applications using the apr library, such as httpd, must be restarted for this update to take effect.

1.4. AUTHCONFIG

1.4.1. RHEA-2011:1003: authconfig enhancement update

Updated authconfig packages that add an enhancement are now available for Red Hat Enterprise Linux 5.

The authconfig packages contain a program with both a command line and a GUI interface for configuring a system to use shadow passwords, or to function as a client for certain network user-information and authentication schemes.

This update adds the following enhancement:

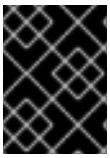
* This update adds the new '--enablesssd' and '--enablesssdauth' command line switches. These options allow administrators to configure the nsswitch.conf and system-auth configuration files so that the System Security Services Daemon (SSSD) is used for account database lookups and authentication. Note, that configuration of the SSSD itself is not handled by authconfig and must be done by other means. (BZ#629021)

All authconfig users are advised to upgrade to these updated authconfig packages, which add this enhancement.

1.5. AUTOFS

1.5.1. RHBA-2011:1079: autofs bug fix and enhancement update

An updated autofs package that fixes several bugs and adds various enhancements is now available for Red Hat Enterprise Linux 5.



IMPORTANT

This update was released as errata RHBA-2011:1079 – autofs bug fix and enhancement 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.

Bug Fixes:

BZ#519281

Prior to this update, the **autofs** utility did not reset the map entry status on a reload request. As a result, newly added map entries that had previously recorded a mount failure failed to work. With this update, **autofs** resets the map entry status on a reload request and map entries are mounted as expected.

BZ#54613

Prior to this update, reloading an existing map could consume an extensive amount of memory. This occurred because the automount daemon failed to free the memory which it preliminary allocated

to the map before it had detected that the map already existed. With this update, the memory is freed and the memory leak no longer occurs on map reload.

BZ#549607

The autofs daemon failed to mount hidden Windows shares when using the auto.smb program map. This occurred because the program map did not translate the $ sign in the share names correctly. With this update, the code that matches the share names has been added and the hidden shares are mounted as expected.

BZ#551599

Prior to this update, the autofs utility could terminate with a segmentation fault when attempting certain mounts. This occurred due to a race condition between mount handling threads for mounts that had previously recorded a mount failure. This update adds a check that verifies that the automount cache map entry is valid and the error no longer occurs.

BZ#559796

The autofs utility failed to mount folders from Windows Server with the ampersand (&) in their name. With this update, such folders are mounted successfully.

BZ#560124

Prior to this update, the automount(8) man page referred to a non-existent man page. This was caused by a typographical error in the code. With this update, the man page reference has been corrected and the man page is displayed as expected.

BZ#561213

Due to a deadlock, autofs could stop responding when attempting to mount map entries that were nested within maps. With this update, the underlying code has been changed and, where possible, nested map entries mount correctly.

BZ#562703

Prior to this update, automount could terminate unexpectedly with a pthreads error. This occurred because attempts to acquire the master map lock occasionally failed as the lock was held by another thread. With this update, the underlying code has been adapted to wait for a short time before failing.

BZ#563956

Previously, the **automount** daemon did not support receiving paged results from an LDAP (Lightweight Directory Access Protocol) server. This update adds the code that handles paged results and such results are processed correctly.

BZ#570783

Prior to this update, if a key entry of an automount map began with an asterisk (*) sign, the daemon failed with a segmentation fault because the sign was not matched correctly. With this update, such asterisk signs are handled correctly.

BZ#576775

Prior to this update, a race condition could have caused the automount daemon to terminate unexpectedly. This happened because the **parse_sun** module pre-opened and cached the Network File System (NFS) mount module so that the mount module could be accessed by other modules

quickly. With this update, the underlying code has been changed and the race condition on longer occurs.

BZ#589573

Prior to this update, the automount daemon stopped responding on startup when started with an already-mounted CIFS (Common Internet File System) share due to a deadlock. With this update, the underlying code has been changed and the deadlock no longer occurs.

BZ#593378

Prior to this update, automount failed to look up mounts from multiple included map sources. This occurred due to a problem with negative caching. With this update, the underlying code has been changed and automount performs the included map lookups correctly.

BZ#601935

When mounting new mounts, the automount daemon could have stopped responding. This occurred due to an execution order race during expire thread creation. This update refactors the code handling expire thread creation and the problem no longer occurs.

BZ#632006

The autofs utility failed to mount Lustre metadata target (MDT) failover mounts because it could not understand the mount point syntax. With this update, the mount point syntax is processed correctly and the failover is mounted as expected.

BZ#632471

Prior to this update, autofs failed occasionally to reload an updated map correctly when the map type was specified explicitly. This occurred because the map stale flag was cleared after the map entry lookup instead of being cleared at the update completion. With this update, the underlying code has been changed to clear the stale flag at the completion of the update and the maps are reread correctly.

BZ#667273

Previously, autofs could have terminated unexpectedly with a segmentation fault if it was heavily loaded with mount requests to service. This occurred due to an invalid pointer. With this update, the underlying code has been changed and autofs no longer crashes in such circumstances.

BZ#668354

Previously, when expanding the & character on map key substitution, autofs handled the white space characters in the key incorrectly. With this update, the underlying code has been changed and the expanding of such keys is handled correctly.

BZ#692524

Previously, autofs could have terminated unexpectedly with a segmentation fault when reloading maps. This occurred when the master map referenced null maps. This error has been fixed, and autofs no longer crashes when reloading such maps.

Enhancements:

BZ#579312

The automount daemon now supports LDAP simple authenticated binds.

BZ#538408

This update adds the `--dumpmaps` option to the `automount` command, which allows you to dump the maps from their source as seen by the automount daemon.

BZ#547510

Previously, if multiple mount locations were present, the selection of a mount depended on the weight value defined by the user and on the server response time. With this update, the user can use the option `--use-weight-only` to make the selection priority depend only on the weight value.

BZ#566481

The autofs utility did not allow the locality name attribute (l) for an LDAP DN (Distinguish Name) in master map entries. This update adds the code to allow the use of DNs with the locality attribute in their name.

BZ#607785

With this update, the autofs utility supports SASL (Simple Authentication and Security Layer) external authentication with certificates using maps stored on an LDAP server.

BZ#610266

This update adds simple Base64 encoding for LDAP and thus allows hashing of the password entries in the `/etc/autofs_ldap_auth.conf` configuration file.

BZ#629357

The autofs utility now provides IP addresses for map entries that use host names with multiple network addresses in its debugging output.

All users of autofs are advised to upgrade to this updated package, which resolves these issues and adds these enhancements.

1.5.2. RHBA-2011:0487: autofs bug fix update

An updated autofs package that fixes a bug is now available for Red Hat Enterprise Linux 5.

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 autofs package fixes the following bug:

* By default, Windows Active Directory servers restrict the number of results that can be retrieved by a single query. If a query returns more than the maximum number of results (1000 by default), the query fails. In such a case, the server returns the results in sets of a specific size (maximum result set size). The automount daemon crashed due to a segmentation fault when it attempted to read a map that contained more results than the maximum result set size. With this update, the automount daemon correctly reads results from larger maps and a segmentation fault no longer occurs. (BZ#691311)

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

1.6. AVAHI

1.6.1. RHSA-2011:0436: Moderate avahi security update

Updated avahi 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 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.

Avahi is an implementation of the DNS Service Discovery and Multicast DNS specifications for Zero Configuration 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, view printers to print to, and find shared files on other computers.

A flaw was found in the way the Avahi daemon (avahi-daemon) processed Multicast DNS (mDNS) packets with an empty payload. An attacker on the local network could use this flaw to cause avahi-daemon on a target system to enter an infinite loop via an empty mDNS UDP packet. (CVE-2011-1002)

All users are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. After installing the update, avahi-daemon will be restarted automatically.

1.7. BASH

1.7.1. RHSA-2011:1073: Low bash security, bug fix, and enhancement update

An updated bash package that fixes one security issue, several bugs, and adds one enhancement is 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.

Bash is the default shell for Red Hat Enterprise Linux.

It was found that certain scripts bundled with the Bash documentation created temporary files in an insecure way. A malicious, local user could use this flaw to conduct a symbolic link attack, allowing them to overwrite the contents of arbitrary files accessible to the victim running the scripts. (CVE-2008-5374)

This update fixes the following bugs:

* When using the source builtin at location ".", occasionally, bash opted to preserve internal consistency and abort scripts. This caused bash to abort scripts that assigned values to read-only variables. This is now fixed to ensure that such scripts are now executed as written and not aborted. (BZ#448508)

* When the tab key was pressed for auto-completion options for the typed text, the cursor moved to an unexpected position on a previous line if the prompt contained characters that cannot be viewed and a "\]". This is now fixed to retain the cursor at the expected position at the end of the target line after autocomplete options correctly display. (BZ#463880)

* Bash attempted to interpret the NOBITS .dynamic section of the ELF header. This resulted in a "^D: bad ELF interpreter: No such file or directory" message. This is fixed to ensure that the invalid "^D" does not appear in the error message. (BZ#484809)

* The $RANDOM variable in Bash carried over values from a previous execution for later jobs. This is fixed and the $RANDOM variable generates a new random number for each use. (BZ#492908)

* When Bash ran a shell script with an embedded null character, bash's source builtin parsed the script incorrectly. This is fixed and bash's source builtin correctly parses shell script null characters. (BZ#503701)

* The bash manual page for "trap" did not mention that signals ignored upon entry cannot be listed later. The manual page was updated for this update and now specifically notes that "Signals ignored upon entry to the shell cannot be trapped, reset or listed". (BZ#504904)

* Bash's readline incorrectly displayed additional text when resizing the terminal window when text spanned more than one line, which caused incorrect display output. This is now fixed to ensure that text in more than one line in a resized window displays as expected. (BZ#525474)

* Previously, bash incorrectly displayed "Broken pipe" messages for builtins like "echo" and "printf" when output did not succeed due to EPIPE. This is fixed to ensure that the unnecessary "Broken pipe" messages no longer display. (BZ#546529)

* Inserts with the repeat function were not possible after a deletion in vi-mode. This has been corrected and, with this update, the repeat function works as expected after a deletion. (BZ#575076)

* In some situations, bash incorrectly appended "/" to files instead of just directories during tab-completion, causing incorrect auto-completions. This is fixed and auto-complete appends "/" only to directories. (BZ#583919)

* Bash had a memory leak in the "read" builtin when the number of fields being read was not equal to the number of variables passed as arguments, causing a shell script crash. This is fixed to prevent a memory leak and shell script crash. (BZ#618393)

* /usr/share/doc/bash-3.2/loadables in the bash package contained source files which would not build due to missing C header files. With this update, the unusable (and unbuildable) source files were removed from the package. (BZ#663656)

This update also adds the following enhancement:

* The system-wide "/etc/bash.bash_logout" bash logout file is now enabled. This allows administrators to write system-wide logout actions for all users. (BZ#592979)

Users of bash are advised to upgrade to this updated package, which contains backported patches to resolve these issues and add this enhancement.

1.8. BIND

1.8.1. RHSA-2011:0926: Important bind security update

Updated bind and bind97 packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

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.

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 discovered in the way BIND handled certain DNS requests. A remote attacker could use this flaw to send a specially-crafted DNS request packet to BIND, causing it to exit unexpectedly due to a failed assertion. (CVE-2011-2464)

Users of bind97 on Red Hat Enterprise Linux 5, and bind on Red Hat Enterprise Linux 6, are advised to upgrade to these updated packages, which resolve this issue. After installing the update, the BIND daemon (named) will be restarted automatically.

1.8.2. RHSA-2011:0845: Important bind security update

Updated bind and bind97 packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

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.

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.

An off-by-one flaw was found in the way BIND processed negative responses with large resource record sets (RRSets). An attacker able to send recursive queries to a BIND server that is configured as a caching resolver could use this flaw to cause named to exit with an assertion failure. (CVE-2011-1910)

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

1.9. BIND97

1.9.1. RHBA-2011:0510: bind97 fix and enhancement update

Updated bind97 packages that fix a bug and add an enhancement are now available for Red Hat Enterprise Linux 5.

The Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) protocols. It contains a DNS server (named), a resolver library with routines for applications to use when interfacing with DNS, and tools for verifying that the DNS server is operating correctly. This package contains version 9.7 of the BIND suite.

These updated bind97 packages fix the following bug:

* BIND could have failed to return queries for subdomains under a newly-added DS (Delegation Signer) record. This occurred because the named daemon failed to validate the new DS record, which was inserted into a trusted DNSSEC (Domain Name System Security Extensions) validation tree. With this update, the daemon validates new DS records correctly. (BZ#695381)

In addition, these updated bind97 packages provide the following enhancement:

* Previously, bind97 did not contain the root zone DNSKEY. DNSKEY is now located in /etc/named.root.key. (BZ#695382)

Users are advised to upgrade to these updated bind97 packages, which resolve this issue and add this enhancement.

1.10. BOOTY

1.10.1. RHBA-2011:0983: booty bug fix update

An updated booty package that fixes various bugs is now available for Red Hat Enterprise Linux 5.

The booty package provides a small python library which is used to create boot loader configuration files for the Anaconda and up2date utilities.

This updated package includes fixes for the following bugs:

* The Anaconda utility incorrectly installed GRUB (GRand Unified Bootloader) on md RAID devices. According to the Anaconda's old setting, GRUB was installed to look for a boot configuration on the hard disk it was running on. When RAID-1 (disk mirroring) was configured and the first hard drive failed, the system was unable to continue the boot process. This could have happened because the second hard drive became the new first hard drive but GRUB was still looking for the second hard drive to boot from. This problem has been fixed and GRUB is now installed correctly and refers to the right hard drive to boot from when one of mirrors is lost. (BZ#213578)

* When a multipath device (mpath) name ended with a digit (for example: rootpvp1), the Kickstart installation failed with a traceback report. This was caused by an error in the mpath device name parser. This issue has been fixed and a verification mechanism has been added to validate the mpath name. The booty package now recognizes more mpath names and the installation fails with an explanation if an invalid mpath name has been used. (BZ#572862)

* Prior this update, booty did not translate physical device names correctly for md software RAID on dm devices (device-mapper subsystem devices), which caused booty to crash during an installation. This issue has been fixed, physical device names are translated correctly and booty no longer crashes in this case. (BZ#667014)

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

1.11. BRIDGE-UTILS

1.11.1. RHEA-2011:1061: bridge-utils enhancement update

An enhanced bridge-utils package is now available for Red Hat Enterprise Linux 5.

The bridge-utils package contains utilities for configuration of the Linux Ethernet bridge. The Linux Ethernet bridge can be used to connect multiple Ethernet devices together. This connection is fully transparent: hosts connected to one Ethernet device see hosts connected to the other Ethernet devices directly.

This updated bridge-utils package adds the following enhancement:

* Support for Internet Group Management Protocol (IGMP) snooping configuration has been added, which allows multicast packets to be forwarded to only relevant interfaces. (BZ#574466)

All users of bridge-utils are advised to upgrade to this updated package, which adds this enhancement.

1.12. BUSYBOX

1.12.1. RHBA-2011:0815: busybox bug fix update

Updated busybox packages that fix multiple bugs are now available for Red Hat Enterprise Linux 5.

busybox is a single binary that includes versions of a large number of system commands, including a shell. This can be very useful for recovering from certain types of system failures, particularly those involving broken shared libraries.

[Updated 2 June 2011] This update fixes a regression in the original fix in which the msh applet was incorrectly executing while loop with empty body. It never exited the loop even if the loop condition was false. With this update, this loop construct works correctly. (BZ#708942)

The original errata update also fixed the following three bugs:

* The grep applet was ignoring the "-i" command line option if the "-F" option was also used. Consequent to this, the "grep -iF" command incorrectly performed a case sensitive search instead of the case insensitive one. This update resolves the problem by ensuring that this combination of command line options works as expected. (BZ#608927)

* Previously, the msh applet had a severely limited depth of shell source operations (that is, the ". FILE" built-in commands). Under certain circumstances, this may have caused it to terminate unexpectedly with the "Shell input nested too deeply" error message. With this update, the maximum number of nested source operations is limited only by the number of available file descriptors and the amount of available memory. (BZ#556845)

* Prior to this update, the msh applet had a limited buffer for the storage of the results of a process substitution. Consequent to this, an attempt to execute certain constructs (for example, `cat FILE` with a file larger than 15KB) could cause it to exit with the "out of string space" error message. With this update, the buffer size is now limited only by the amount of available memory. (BZ#678701)

Users are advised to upgrade to these updated busybox packages, which fix these bugs.

1.13. CERTMONGER

1.13.1. RHBA-2011:1002: certmonger bug fix and enhancement update

An updated certmonger package that fixes multiple bugs and adds several enhancements is now available for Red Hat Enterprise Linux 5.

The certmonger package contains a service which is primarily concerned with getting your system enrolled with a certificate authority (CA) and keeping it enrolled.

The certmonger package has been upgraded to upstream version 0.42, which provides a number of bug fixes and enhancements over the previous version. (BZ#688610)

Additionally, this update fixes the following bugs:

* Previously, when issuing a request for a certificate to an IPA server, if the IPA server returned an error, the ipa-submit helper process terminated unexpectedly while attempting to parse the error in order to report it. The bug has been fixed in this update, and the error is now recorded properly. (BZ#690892)

* Previously, if certmonger did not track any certificates, the output of the "ipa-getcert list" command was empty. This undesired behavior has been fixed so that after running the command, the number of the certificates tracked is now displayed as well as any certificate entries, if they exist. (BZ#681642)

* Previously, when the service attempted to save a certificate to a certificate database, if there was already a certificate in the database with the desired nickname assigned to it but which had a different

value in its "subject name" field, the attempt to save the new certificate to the database failed. This bug has been fixed in this update so that any certificates that are already in the certificate database which have the desired nickname are now cleared out before attempting to store a new certificate, and storing the new certificate no longer fails. (BZ#695717)

* Previously, when a non-root user ran the "ipa-getcert" command, an unclear and ambiguous error message about insufficient user rights to run the command was displayed. This update improves the error message text so that it is now clear and straightforward. (BZ#681641)

* Previously, building the certmonger package failed due to a problem with self-tests. This problem has been resolved and does not occur anymore. (BZ#670322)

All users requiring certmonger should upgrade to this updated package, which fixes these bugs and adds several enhancements.

1.14. CMAN

1.14.1. RHBA-2011:1001: cman bug fix and enhancement update

Updated cman package that fixes bugs and adds enhancements is now available for Red Hat Enterprise Linux 5.

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

This update applies fixes for the following bugs:

* It is now possible to make ccs_tool use different ports. (BZ#656427)

* The fence_cisco_ucs agent now supports sub organizations. (BZ#678902)

* "cman_tool nodes -F id,type,name,addr" no longer crashes when qdisk is enabled. (BZ#654894)

* cman_tool now displays node votes. (BZ#653508)

* Manual pages for fencing agents have been brought up to date. (BZ#488959, BZ#573990, BZ#663808, BZ#671089)

* fence_wti now works with larger (>16) port switches. (BZ#679160)

* A timing issue causing erratic qdiskd heuristic behavior has been fixed. (BZ#679274)

* A traceback in fence_rsa has been fixed. (BZ#678018)

In addition, this update adds the following enhancements:

* There is now a "diag" option to fence_ipmilan to support ipmi chassis power diag. (BZ#678061)

* The fence_rhevm agent has been updated to match the current REST API. (BZ#681670, BZ#681676)

* The fence_vmware agent has been rewritten to use the VMWare SOAP API. (BZ#634567)

* cman_tool no longer reports an incorrect node count. (BZ#649533)

* The man page documentation for the "expected" option to cman_tool has been improved. (BZ#688701)

* The --ssl option now works with fence_cisco_ucs. (BZ#693395)

* "fence_ipmilan -o monitor" now returns the correct status if the chassis is powered off. (BZ#693427)

All cman users are advised to upgrade to this updated package, which fixes these issues and add these enhancements.

1.14.2. RHBA-2011:0006: cman bug fix and enhancement update

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 fixes the following bug:

* Previously, no manual pages were available for the new agents fence_cisco_ucs, fence_rhevm, and fence_ifmib. This update adds these manual pages. (BZ#664381)

All cman users are advised to upgrade to this update, which resolves this issue.

1.14.3. RHBA-2011:0470: cman bug fix update

An updated cman package that fixes one bug is now available for Red Hat Enterprise Linux 5.

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

This update fixes the following bug:

* Previous versions of the ccs_tool utility did not allow users to specify the port numbers to use when distributing the configuration. Consequent to this, changing the port numbers for Cluster Manager components rendered this utility unable to establish a connection with a cluster. With this update, the ccs_tool utility now allows users to specify the port numbers on the command line, so that the connection can be established as expected. (BZ#677814)

All users of cman are advised to upgrade to this updated package, which fixes this bug.

1.14.4. RHBA-2011:0900: cman bug fix update

An updated cman package that fixes one bug is now available for Red Hat Enterprise Linux 5.

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

This update fixes the following bug:

* Previously, quorum disk heuristic timers in a cluster functioned improperly. As a consequence, if the heartbeat network malfunctioned, the cluster nodes could end up fencing each other in a non-deterministic way. With this update, the problem with the timers has been addressed and the bug no longer occurs. (BZ#707053)

All users of cman are advised to upgrade to this updated package, which fixes this bug.

1.15. CONGA

1.15.1. RHSA-2011:0394: Important conga security update

Updated conga 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 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.

The conga packages provide a web-based administration tool for remote cluster and storage management.

A privilege escalation flaw was found in luci, the Conga web-based administration application. A remote attacker could possibly use this flaw to obtain administrative access, allowing them to read, create, or modify the content of the luci application. (CVE-2011-0720)

Users of Conga are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing the updated packages, luci must be restarted ("service luci restart") for the update to take effect.

1.15.2. RHBA-2011:1039: conga bug fix and enhancement update

Updated conga packages that fix multiple bugs and introduce feature enhancements are now available for Red Hat Enterprise Linux 5.

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 fixes the following bugs:

* Prior to this update, the luci_admin utility did not operate correctly if third-party packages of the Zope web application server were installed on the system. With this update, this issue has been fixed so that the luci_admin utility now works as expected. (BZ#643996)

* Prior to this update, the length of certain text fields in luci's resource agent forms was insufficient, causing the inability to see the whole text field content. The problem has been resolved in this update by increasing the length of the respective text fields. (BZ#640329)

* Prior to this update, managing a cluster that contained a large number of services or resources configured in the /etc/cluster/cluster.conf file resulted in a "RuntimeError: maximum recursion depth exceeded" error message if a user tried to display that particular cluster. This problem has been resolved so that cluster management works as expected, and no error message is displayed when viewing the cluster. (BZ#658621)

As well, this update adds the following enhancements:

* The commands issued with luci and run by ricci are now logged using the system log facility so that it is now easier to debug problems with Conga actions. (BZ#459190)

* Support for specifying a sub-organization for the fence_cisco_ucs I/O Fencing agent has been added in this update. (BZ#690936)

* Support for setting the "self_fence" attribute for Highly Available Logical Volume Management (HA LVM) resources has been added with this update. (BZ#679866)

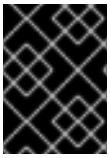
* Support for configuring the new fence_vmware_soap Fencing agent has been added in this update. (BZ#705073)

All Conga users are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

1.16. COREUTILS

1.16.1. RHBA-2011:1074: coreutils bug fix and enhancement update

An updated coreutils package that fixes number of bugs and adds various enhancements is now available for Red Hat Enterprise Linux 5.



IMPORTANT

This update was released as errata RHBA-2011:1074 — coreutils bug fix and enhancement update.

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

Bug Fixes:

BZ#510809

When a directory contained a symbolic link to itself, the **readlink** command incorrectly gave the following error message:

```
Too many levels of symbolic links.
```

With this update, the **readlink** command is able to correctly resolve values of recursive symbolic links to directories and no error messages are given.

BZ#684249

When values of **LC_TIME** and **LC_CTYPE** variables differed, the **sort** utility sometimes terminated due to an assertion failure. This bug has been fixed and the **sort** utility no longer crashes in the described scenario.

BZ#559098

When a child process was terminated by a signal, the **su** utility returned the wrong exit code of 0, which means exit success. With this update, the **su** utility always returns the correct exit code in the described scenario.

BZ#668247

Previously, when the **dd** utility read data from a pipe and received a signal such as **SIGPIPE**, it stopped reading the current block and started with the new one immediately. This caused random output values when the **dd** utility was used to measure the size of an input file. With this update, the new **iflag=fullblock** option is available. When the option is used, the **dd** utility always continues to read incomplete blocks after receiving a signal.

BZ#664895

On certain file systems such as VxFS, the Veritas File System, the **rmdir()** system call returned the wrong error code for non-empty directories. This caused the rmdir utility to fail to ignore the error when the **--ignore-fail-on-non-empty** command line option was specified. This bug has

been fixed and the **rmdir** utility now handles errors on non-empty directories on VxFS partitions properly.

BZ#515499

Previously, when the `ls -1U` command was called with two or more arguments and with at least one non-empty directory as an argument, directory entry names were printed before the name of their parent directories. This bug has been fixed and now the entries are printed in correct order.

BZ#525199

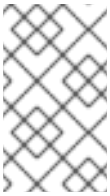
Previously, the **cp**, **mv** and **install** utilities were unable to preserve extended attributes on files with read-only permissions. This bug has been fixed and the extended attributes are now preserved correctly by those utilities.

BZ#537463

If the `--ghost` option was enabled for an automount point, the **du** command failed on an automounted directory if it was not mounted yet. This bug has been fixed and the **du** command now succeeds on an automounted directory on the first attempt.

BZ#520630

Due to a regression, running the `df -l` command with a specific device specified resulted in a `Permission denied` error message for regular users. This bug has been fixed and specifying a device now works for regular users.



NOTE

Note that running the `df -l` command 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#628953

Because of internal reordering of arguments, the **runcon** utility was not able to handle execution of commands with arguments without the option separator `--`. With this update, the **runcon** utility no longer reorders arguments and this bug no longer occurs.

NOTE

Note that syntax `runcon RUNCONARGS COMMAND -- COMMANDARGS` is incorrect; if the option separator is used, it must precede the `COMMAND`.

BZ#627285

Previously, the `--backup` option of the `mv` command did not work with directories and the `cannot move [directory] to a subdirectory of itself` error message was returned. This bug has been fixed and the `--backup` option now works with directories as expected.

BZ#524805

Previously, the **runuser** utility man page contained incorrect information about PAM API calls. With this update, the documentation has been amended.

BZ#586957

Previously, certain scripts parsing the **LS_COLORS** environment variable used insufficient escaping, resulting in slow shell start-up in directories with too many files. This bug has been fixed and the shell start-up time is now more independent of the current directory.

BZ#658839

When moving a directory into another non-empty directory, the **mv** utility returned a confusing **`cannot move [directory] to a subdirectory of itself`** error message. This bug has been fixed and the correct **`Directory not empty`** error message is now returned instead.

BZ#681598

Previously, due to a bug in the **su** utility, the **suspend** command did not work for root users in **`tcsh`** shell. With this update, when the **suspend** command is called in a root shell, the **`Suspended (signal)`** message is returned and the user is put back into their user shell.

Enhancements:

BZ#584802, **BZ#610559**, **BZ#660186**

This update improves the coreutils documentation in the following ways: descriptions of the **runcon** and **chcon** utilities have been added; the behavior of newly added groups is now described; and the description of the **`mkdir --mode`** command has been extended.

BZ#523923

Previously, deletion of a large number of files via the **rm** utility was taking too much time. With this update, the code has been optimized and the deletion is now faster.

BZ#513153

With this update, many unnecessary warning messages of attempts for preserving ACLs on file systems without the support for ACLs have been suppressed, unless the preservation of ACLs is explicitly requested.

BZ#582774

With this update, the **`-L`** (logical) and **`-P`** (physical) command line options are now supported. These options are used for resolving the path of current working directory.

All coreutils users are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

1.16.2. RHBA-2011:0188: coreutils bug fix update

An updated coreutils package that fixes a bug is now available for Red Hat Enterprise Linux 5.

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 "su" utility, which switches the user, does not return exit code of the child process command, if the child process is terminated by a signal. Returned exit code 0 - which means exit success - could be confusing for scripts. With this updated package, correct exit code is returned, thus resolving the issue.

(BZ#672863)

All users of coreutils should upgrade to this updated package, which resolves this issue.

1.16.3. RHEA-2011:0165: coreutils enhancement update

An updated coreutils package that adds an enhancement to dd 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 adds the following enhancement:

* When a dd command copies data and receives e.g. SIGPIPE signal, then it stops with the current block (leaving it as partial) and starts with the new one, which is called "short read". Sometimes it is useful that dd has to copy full blocks and not stop reading after received signals. To address this, dd now accepts iflag=fullblock, to make it accumulate full input blocks. With this new option, after a short read, dd repeatedly calls read, until it fills the incomplete block, reaches EOF, or encounters an error. (BZ#668465)

All coreutils users may upgrade to this updated package, which adds this enhancement.

1.17. CPUSPEED

1.17.1. RHBA-2011:0502: cpuspeed bug fix update

An updated cpuspeed package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The cpuspeed daemon manages the CPU frequency scaling.

This update fixes the following bug:

* The /etc/sysconfig/cpuspeed configuration file allows a user to specify custom maximum (the "MAX_SPEED" option) and minimum (the "MIN_SPEED" option) clock speed limits. Prior to this update, when a user removed these custom settings from the configuration and restarted the service, the cpuspeed init script failed to reset these values to the hardware-specific limits. With this update, the init script has been adapted to ensure that when the minimum or maximum clock speed value is not specified, cpuspeed correctly uses the value reported by the CPU. (BZ#616524)

All users of cpuspeed are advised to upgrade to this updated package, which fixes this bug.

1.18. CRYPTSETUP-LUKS

1.18.1. RHBA-2011:0987: cryptsetup-luks bug fix update

An updated cryptsetup-luks package that fixes various bugs is now available for Red Hat Enterprise Linux 5.

The cryptsetup-luks package provides a utility for setting up encrypted file systems using Device Mapper and the dm-crypt target.

This updated cryptsetup-luks package includes fixes for the following bugs:

* When executing the "cryptsetup luksOpen" command on an encrypted disk device formatted with an

older version of cryptsetup, the following message appeared: "automatic header conversion from 0.99 to 0.991 triggered". Consequently, the device became unresponsive at every attempt to open it. The older version of cryptsetup converted the master key iteration count incorrectly, which has been fixed and the device hangs no longer. (BZ#583431)

* The cryptsetup utility became unresponsive when using the "cryptsetup isLuks" command on an ordinary file. This problem has been fixed: if running the command on an ordinary file, the cryptsetup utility informs users about the file not being a LUKS partition. (BZ#622712)

* Previously, the cryptsetup utility could have terminated unexpectedly when the key size was larger than 256 bits. The cryptsetup utility now properly supports keys longer than 256 bits, fixing the problem. (BZ#678011, BZ#684616)

* When removing a key from the key slot by running the "cryptsetup luksDelKey" command, only the key slot itself was cleared but the salt and iteration count remained in the key slot header. All additional information is now cleared as well. (BZ#697815)

All users of cryptsetup-luks are advised to upgrade to this updated package, which resolves these bugs.

1.19. CUPS

1.19.1. RHBA-2011:0185: cups bug fix update

Updated cups packages that fix a bug are now available for Red Hat Enterprise Linux 5.

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

This update fixes the following bug:

* Previously, when the cupsd daemon was running with SELinux features enabled, file descriptor count was increasing over time until resources ran out. With this update, resources are allocated only once. (BZ#670909)

Users of CUPS are advised to upgrade to these updated packages, which resolve this issue. After installing this update, the cupsd daemon will be restarted automatically.

1.20. CURL

1.20.1. RHSA-2011:0918: Moderate curl security update

Updated curl packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

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 provides the libcurl library and a command line tool for downloading files from servers using various protocols, including HTTP, FTP, and LDAP.

It was found that cURL always performed credential delegation when authenticating with GSSAPI. A rogue server could use this flaw to obtain the client's credentials and impersonate that client to other servers that are using GSSAPI. (CVE-2011-2192)

Users of curl should upgrade to these updated packages, which contain a backported patch to correct this issue. All running applications using libcurl must be restarted for the update to take effect.

1.20.2. RHBA-2011:0179: curl bug fix update

An updated curl package that fixes a bug is now available for Red Hat Enterprise Linux 5.

cURL is a tool for getting files from FTP, HTTP, Gopher, Telnet, and DICT servers, using any of the supported protocols. It is designed to work without user interaction or any kind of interactivity, and offers many useful capabilities such as proxy support, user authentication, FTP upload, HTTP post, and file transfer resume.

This update fixes the following bug:

* Previously, an attempt to send an LDAP request through an HTTP proxy tunnel ended up with cURL trying to connect to the LDAP server directly using a wrong port number. With this update, the underlying source code has been modified to address this issue, and cURL now works as expected. (BZ#670523)

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

1.21. CYRUS-IMAPD

1.21.1. RHSA-2011:0859: Moderate cyrus-imapd security update

Updated cyrus-imapd packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

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

It was discovered that cyrus-imapd did not flush the received commands buffer after switching to TLS encryption for IMAP, LMTP, NNTP, and POP3 sessions. A man-in-the-middle attacker could use this flaw to inject protocol commands into a victim's TLS session initialization messages. This could lead to those commands being processed by cyrus-imapd, potentially allowing the attacker to steal the victim's mail or authentication credentials. (CVE-2011-1926)

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

1.21.2. RHBA-2011:1075: cyrus-imapd bug fix update

Updated cyrus-imapd packages that fix multiple bugs are now available for Red Hat Enterprise Linux 5.

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

This update fixes the following bugs:

* Prior to this update, cyrus-imapd cleared its back end before deinitialization. As a result, when the "unselect" command was used in proxy mode, cyrus-imapd terminated unexpectedly. This bug has been fixed in this update so that cyrus-imapd now clears the back end after deinitialization, and the "unselect" command can be used properly in proxy mode as expected. (BZ#679253)

* Prior to this update, the "ignorequota" command did not work on 64-bit systems. As a result, despite using the "ignorequota" command, it was not possible to deliver a mail message to a user whose quota exceeded the quota limit. This bug has been fixed in this update so that the "ignorequota" command now works on 64-bit systems, as expected. (BZ#584088)

* Prior to this update, Python files included in the cyrus-imapd packages contained the "#!/usr/bin/env python" string. With this update, the string in the aforementioned files has been modified to "#!/usr/bin/python" so that another version of Python can now be installed as expected. (BZ#521338)

* Prior to this update, the cyrus-imapd packages required the lm_sensors-devel package at build time. The lm_sensors-devel package is not available on all platforms supported by Red Hat Enterprise Linux 5. As a result, a very complex spec file had to be distributed with the cyrus-imapd packages. With this update, this bug has been fixed in this update so that the cyrus-imapd packages now require only the net-snmp-devel package, which already solves the lm_sensors package requirement. (BZ#437999)

* Prior to this update, cyrus-imapd did not close all file descriptors that were used for quota. As a result, after moving several folders, cyrus-imapd could have used up available file descriptors and could have not been able to function properly. With this update, cyrus-impad now closes all quota descriptors when they are no longer required, as expected. (BZ#253854)

All users are advised to upgrade to these updated cyrus-imapd packages, which fix these bugs.

1.22. DAPL

1.22.1. RHBA-2011:0371: dapl bug fix update

Updated dapl packages that fix a bug are now available for Red Hat Enterprise Linux 5.

The dapl package provides a user-space implementation of the DAT 2.0 API that allows applications to utilize high-performance network technologies such as InfiniBand and iWARP.

This update fixes the following bug:

* Due to an invalid error mapping, when dapl received a signal during the execution of the dapls_evd_dto_wait() function, it could fail to set the correct error type, which may have led to an incorrect operation. With this update, the relevant part of the source code has been modified to return the correct value, and dapl now works as expected. (BZ#660256)

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

1.23. DBUS

1.23.1. RHSA-2011:0376: Moderate dbus security update

Updated dbus packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

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.

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.

A denial of service flaw was discovered in the system for sending messages between applications. A local user could send a message with an excessive number of nested variants to the system-wide message bus, causing the message bus (and, consequently, any process using libdbus to receive messages) to abort. (CVE-2010-4352)

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.

1.24. DEJAGNU

1.24.1. RHBA-2011:0399: dejagnu bug fix update

An updated dejagnu package that fixes one bug is now available for Red Hat Enterprise Linux 5.

DejaGnu is an Expect/Tcl based framework for testing other programs, and provides a single front end for all tests.

This update fixes the following bug:

* Prior to this update, the runtest utility did not reset variables before running a test, causing certain test cases to be incorrectly evaluated as "UNRESOLVED". This update ensures that the variables are properly reset before a test is run, and all test cases are now evaluated correctly. (BZ#460153)

All users of dejagnu are advised to upgrade to this updated package, which fixes this bug.

1.25. DEVICE-MAPPER

1.25.1. RHBA-2011:0981: device-mapper bug fix and enhancement update

Updated device-mapper packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

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

The device-mapper package has been upgraded to upstream version 1.02.63, which provides a number of bug fixes and enhancements over the previous version. (BZ#680958) Those enhancements include:

* Unlink failure in the remove_lockfile() function in dmeventd is now checked for.

* Inactive table query support is now supported when using the Red Hat Enterprise Linux 5.7 kernel. The "dmsetup table --inactive" command can be run to view the contents of the inactive table instead of the live one, which is the default.

* The dm_task_secure_data() function has been added to libdevmapper to wipe the ioctl buffers in the kernel.

* A new "-R" option has been added to restart dmeventd without loss of state.

These updated device-mapper packages provide fixes for the following bugs:

* Previously, booting encrypted devices which used Multi-Level Security (MLS) enforcing mode failed with this error message:

/dev/mapper/temporary-cryptsetup-977: lsetfilecon failed: Operation not permitted

The problem occurred when cryptsetup created a device node and relabeled it using the lsetfilecon() function instead of using the setfscreatecon() function. This has been fixed and devices which used MLS enforcing mode now boot successfully. (BZ#584884)

* When installing the kernel-2.6.18 packages, this error message was logged to the /root/install.log file: "matchpathcon failed: No such file or directory". The problem has been fixed and this error message is no longer logged to install.log with this update. (BZ#695374)

* This update fixes a conflict which occurred when lvm2 and the device mapper debuginfo packages were installed together. (BZ#701715)

Users are advised to upgrade to these updated device-mapper packages, which resolve these bugs and add these enhancements.

1.26. DEVICE-MAPPER-MULTIPATH

1.26.1. RHBA-2011:1032: device-mapper-multipath bug fix and enhancement update

Updated device-mapper-multipath packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

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

This update fixes the following bugs:

* Prior to this update, when viewing partition information from a file, kpartx used a loop device which was not released by kpartx afterwards. With this update, this erroneous behavior has been fixed so that kpartx now correctly releases a loop device as expected. (BZ#578109)

* After a thread of the multipathd service acquired its resource locks, the thread did not check if it had been canceled before accessing the resource. This caused multipathd to occasionally terminate unexpectedly with a segmentation fault on shutdown if the thread attempted to access the resource after the thread was canceled. With this update, the bug has been fixed so that the multipathd thread now checks if it is canceled before accessing its resource. (BZ#639429)

* When the multipathd service started, it created a separate namespace for itself, and unmounted all unnecessary disk-backed file systems. Since /ram file systems are not considered to be disk-backed, they should have not been unmounted by multipathd, however multipathd unmounted them. This update corrects this undesired behavior so that the /ram file systems are no longer unmounted. (BZ#663179)

* Prior to this update, the multipathd service did not check if a value was entered for an option in the /etc/multipath.conf configuration file before attempting to read the value. As a result, multipathd terminated unexpectedly when an option without any value was found in /etc/multipath.conf. With this update, the bug has been fixed so that multipathd no longer crashes. (BZ#675369)

* If the last path of a device was deleted while the multipathd service was trying to reload the device map, or if a ghost path failed, multipathd did not always switch into recovery mode. As a result, multipath devices were not able to recover I/O operations in setups that were supposed to temporarily queue I/O if all paths were unavailable. This update resolves both of these problems; multipath now correctly recovers I/O operations as configured. (BZ#677821)

* Prior to this update, there was a spelling mistake found in the "invalid keyword" error message. The spelling mistake has been fixed in this update. (BZ#676165)

As well, this update adds the following enhancements:

* This update introduces two new defaults options in the /etc/multipath.conf configuration file: "fast_io_fail_tmo" and "dev_loss_tmo". The "fast_io_fail_tmo" option controls how long the SCSI layer waits after a SCSI device fails before failing back the I/O. This option can be set to "off" or any number less than the "dev_loss_tmo" option. The "dev_loss_tmo" option controls how long the SCSI layer waits after a SCSI device fails before marking it as failed. The default values for these options are set by the SCSI device drivers. (BZ#672575)

* This update introduces a new defaults section parameter for the /etc/multipath.conf configuration file: the "file_timeout" parameter. This parameter controls how many seconds the multipathd service will wait for a necessary file to appear while setting up a multipath device. The default value is 90 seconds. (BZ#627911)

* This update introduces the default configuration for multiple new HP storage array products. (BZ#502813)

All users of device-mapper-multipath should upgrade to these updated packages, which fix these bugs and add these enhancements.

1.26.2. RHBA-2011:0322: device-mapper-multipath bug fix update

Updated device-mapper-multipath packages that fix a bug are now available for Red Hat Enterprise Linux 5 Extended Update Support.

The device-mapper-multipath packages provide tools to manage multipath devices by giving the dm-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 fixes the following bug:

* The "dev_loss_tmo" and "fast_io_fail_tmo" sysfs parameters provide a way to customize timeout values in case of a multipath device failure. Prior to this update, the multipathd daemon was unable to set these values, which may have led to performance issues. To prevent this, this update adds support for the "dev_loss_tmo" and "fast_io_fail_tmo" configuration options, which allow users to override default values for the corresponding sysfs parameters. (BZ#678991)

All users of device-mapper-multipath are advised to upgrade to these updated packages, which resolve this issue.

1.26.3. RHBA-2011:0379: device-mapper-multipath bug fix update

Updated device-mapper-multipath packages that resolve an issue are now available for Red Hat Enterprise Linux 5.

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

These updated device-mapper-multipath packages fix the following bug:

* If a device's last path was deleted while the multipathd daemon was trying to reload the device map, or if a ghost path failed, multipathd did not always switch into the recovery mode. As a result, multipath devices could not recover I/O operations in setups that were supposed to temporarily queue I/O if all paths were down. This update resolves both of these issues; multipath now correctly recovers I/O operations as configured. (BZ#683447)

All users of device-mapper-multipath are advised to upgrade to these updated packages, which resolve this issue.

1.26.4. RHBA-2011:0864: device-mapper-multipath bug fix update

Updated device-mapper-multipath packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The device-mapper-multipath packages provide tools to manage multipath devices by giving the "dm-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 fixes the following bug:

* After acquiring their resource locks, multipathd's threads did not check if they were canceled before accessing their resources. This caused multipathd to close with a segmentation fault on shutdown, if a thread attempted to access a resource after it was canceled. Now all multipathd threads check if they are canceled before accessing their resources. (BZ#704470)

All users of device-mapper-multipath are advised to upgrade to these updated packages, which fix this bug.

1.27. DHCP

1.27.1. RHSA-2011:0428: Important dhcp security update

Updated dhcp packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

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.

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.

It was discovered that the DHCP client daemon, dhclient, did not sufficiently sanitize certain options provided in DHCP server replies, such as the client hostname. A malicious DHCP server could send such an option with a specially-crafted value to a DHCP client. If this option's value was saved on the client system, and then later insecurely evaluated by a process that assumes the option is trusted, it could lead to arbitrary code execution with the privileges of that process. (CVE-2011-0997)

Red Hat would like to thank Sebastian Krahmer of the SuSE Security Team for reporting this issue.

All dhclient users should upgrade to these updated packages, which contain a backported patch to correct this issue.

1.27.2. RHBA-2011:1038: dhcp bug fix and enhancement update

Updated dhcp packages that fix several bugs and add an enhancement are now available for Red Hat Enterprise Linux 5.

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. DHCPv6 is the DHCP protocol version for IPv6 networks.

This update fixes the following bugs:

* Previously, the dhcpd service sometimes started to give new leases to clients in the INIT state rather than to presently active clients. That led to premature exhaustion of available leases for new clients. With this update, the server's "by client-id" and "by hardware address" hash table lists are sorted according to the preference to re-allocate the lease to returning clients, and the pool starvation problem no longer occurs in the described scenario. (BZ#615995)

* Previously, moving the server from the "communication-interrupted" state to the "partner-down" state did not force the server to take over the partner's leases. Consequently, clients could not get an IP address from the pool of the previously terminated DHCP server. With this update, a failover server in "partner-down" state is able to re-allocate leases to clients. (BZ#610219)

* Previously, the dhclient utility wasn't requesting the interface-mtu option by default. This caused difficulties when the network configuration changed and the MTU (Maximum Transmission Unit) value needed to be changed on all hosts. With this update, the dhclient utility requests the interface-mtu option by default. (BZ#694264)

* Previously, the dhcpd init script lacked several variables and actions required by the Linux Standard Base (LSB). With this update, the init script has been amended and it is now LSB-compliant. (BZ#610128)

* Previously, when the dhcpd service was used in a failover configuration, the primary server sometimes wrote so many "lease imbalance" messages into its log files, that it resulted in a termination. With this update, these messages are not logged unless rebalance is attempted, and the bug no longed occurs. (BZ#661939)

* Previously, when the system had been rebooted while the network switch had been down, after the network connection was recovered, the network interface configuration was not configured with DHCP, even if the dhclient utility was running in persistent mode. With this update, the dhclient-script file has been amended to refresh the ARP (Address Resolution Protocol) table and the routing table instead of bringing the interface down, which fixes the bug. (BZ#685048)

* Previously, when multiple DHCP clients were launched at the same time to handle multiple virtual interfaces on the same network interface card (NIC), the clients used the same seed to choose when to renew their leases. Consequently, virtual interfaces for some clients could have been deconfigured over time. With this update, the dhclient utility uses the PID (Process Identifier) for seeding the random number generator, which fixes the bug. (BZ#623953)

* Previously, it was impossible to configure the dhcrelay service to run the dhcrelay daemon with additional arguments. With this update, a DHCRELAYARGS variable is available for the /etc/sysconfig/dhcrelay configuration file, which allows additional arguments to be passed to the dhcrelay daemon properly. (BZ#624965)

* There was a small error regarding the dhcp-lease-time option in the dhclient.conf(5) man page. With this update, the man page has been amended. (BZ#585855)

This update adds the following enhancement:

* The dhcp package now provides support for IPoIB (IP over InfiniBand) interfaces. (BZ#660679)

Users of dhcp are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

1.28. DMIDECODE

1.28.1. RHEA-2011:0988: dmidecode enhancement update

An updated dmidecode package that provides one enhancement is now available for Red Hat Enterprise Linux 5.

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.

The dmidecode package has been upgraded to version 2.11, which updates support for SMBIOS specification version 2.7. (BZ#661864)

Users of dmidecode are advised to upgrade to this updated package, which adds this enhancement.

1.29. DMRAID

1.29.1. RHBA-2011:1020: dmraid bug fix update

Updated dmraid packages that fix multiple bugs are now available for Red Hat Enterprise Linux 5.

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

This update fixes the following bugs:

* Prior to this update, the dmeventd-logwatch crontab file was not able to specify the user that the logwatch process should be executed by. Due to this problem, the dmraid logwatch created an incomplete crontab entry. As a workaround, users can now change the functional portion of this crontab to: "* * * * * root /usr/sbin/logwatch --service dmeventd --range today --detail med". (BZ#516892)

* Prior to this update, the operating system did not boot from the RAID volume after an interrupted rebuild operation. Due to this problem, a kernel panic happened during the rebuild process. With this update, the operating system is fully operational after the rebuild. (BZ#626417)

* Prior to this update, Intel ISW RAID was not correctly rebuilt when a fresh disk was replaced in the array set. Due to this behavior, data could become corrupted. With this update, the code is modified so that it inquires the ISW metadata for rebuilding the drive. (BZ#635995)

* Prior to this update, a code path incorrectly dereferenced already known NULL pointers. Due to this problem, dmraid ended with an application coredump. This update adds a check against NULL before the pointer dereference. Now, known NULL pointers are no longer dereferenced. (BZ#696528)

All dmraid users are advised to upgrade to these updated packages, which fix these bugs.

1.30. DOGTAIL

1.30.1. RHBA-2011:0315: dogtail bug fix update

An updated dogtail package that fixes a bug is now available for Red Hat Enterprise Linux 5.

Dogtail is a test tool and automation framework for a graphical user interface (GUI) that uses accessibility technologies to communicate with desktop applications.

This update fixes the following bug:

* Due to a missing pygtk2-libglade runtime dependency, an attempt to run the sniff utility could fail with the following message written to standard error:

ImportError: No module named glade

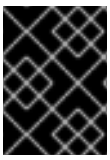
This updated package corrects this dependency, so that the sniff utility no longer fails to run. (BZ#435714)

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

1.31. E2FSPROGS

1.31.1. RHBA-2011:1080: e2fsprogs bug fix and enhancement update

An updated e2fsprogs packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.



IMPORTANT

This update was released as errata RHBA-2011:1080 — e2fsprogs bug fix and enhancement update.

The e2fsprogs packages contain a number of utilities that create, check, modify, and correct inconsistencies in ext2, ext3, and ext4 file systems. This includes e2fsck (which repairs file system inconsistencies after an unclean shutdown), mke2fs (which initializes a partition to contain an empty file system), tune2fs (which modifies file system parameters), and most of the other core file system utilities.

Bug Fixes:

BZ#489842

When lsattr or chattr was pointed at a non-existent file, an error was returned in that the exit code was always zero. This was because ls reported an error if any occurred, and lsattr did the same, reporting the last error encountered. This patch fixes this error, and lsattr and chattr provide the correct error.

BZ#491385

After using resize2fs to perform an offline resize of a file system, running e2fsck gave an error, stating the wrong block count for the resize inode. This was because the resize inode was not being

properly cleared. This patch checks to see if the file system has grown to the point where the resize_inode is no longer needed, then cleans it so e2fsck does not have to. The correct block count is now given for the resize inode.

BZ#506643

Previously, e2fsprogs libblkid probe_all() could mismatch devices when scanning whole disks without partitions where the name ended in a number. This caused a mount failure. With this patch these disks are also scanned, so the devices are mounted correctly.

BZ#553216

When a host was re-kickstarted, mpath mount with LABEL failed with the error “mount: /dev/sdk already mounted or /san/intf busy”. This was because the probe_one() function scanned /dev before /dev/mapper. This patch disables all calls from libdevmapper via #undef HAVE_DEVMAPPER, instead using the standard support for “normal” non-dm devices. This results in mpath can mount without errors.

BZ#562044

Running “e2fsck -y -f” on a corrupted file system printed errors when “e2fsck -y” previous reported the file system to be cleaned of errors. This occurred when a file had its i_file_acl block cloned as a duplicate. This duplicate was then cleared because the file system did not have the xattr feature, and the inode was subsequently removed due to an invalid mode. The second e2fsck pass found the cloned xattr block in use but not owned by any file, so had to fix up the block bitmaps. This patch fixes an existing brace misalignment and skips the processing of the duplicate xattr blocks on a non-xattr file system, as these will be cleaned at a later point, allowing the clean to occur properly.

BZ#579836

On 64-bit system, a sign extension bug in libcom_err caused incorrect error messages to be emitted. This was because an error code as an (int) was passed to error_message as an (unsigned int), especially when using libgssapi_krb5. This meant that error_message() failed to find a matching error table. To fix this, error_message() has been changed to follow the same method error_table_name() does when error_message() calls it. That is, it drops most of the higher bits of the parameter passed before continuing, so now correct error messages are emitted.

BZ#580671

A sparse journal (which indicates corruption) was not fixed by e2fsck, causing file system errors and a shut down after mount. This was because e2fsck marked the file system as clean so it would mount, but did not fix that block, so when the journal reached this point again it failed once more. This patch changes process_journal_block() to clear and recreate the journal inode if it is sparse, that is if it gets block 0, allowing e2fsck to correctly fix a sparse journal.

BZ#606757

Previously, chattr and lsattr would return “error code = 0” even when they have not done anything, which made error checking difficult in scripts. With this patch, if there are errors they will be reported with a non-zero exit code. It will give explicit errors when attempting to set files that are not files or directories (which are not currently supported under Linux). Also, the -f flag will suppress error messages from being printed even though the exit status will still be non-zero.

BZ#607843

When checking a particular volume, e2fsck exited with a signal 11 (segmentation fault). This was caused by floating point errors. This patch edits get_icount_el to prevent point precision errors on large file systems from causing the search interpolation algorithm from performing an infinite loop, allowing e2fsck to check the volume correctly.

BZ#618134

The fsck command returned a 0 status instead of an appropriate error code on an exec() failure, due to an error in the code. This patch fixes the error so that the appropriate error code is now returned.

BZ#637920

Previously, blkid cachine caused a tag search (blkid -l -t ...) to return empty results. This occurred mostly in debug code, where dev->bid_type is not-NULL before dereferencing the pointer. This has been edited and blkid cachine now returns proper results.

BZ#669676

Previously, e2fsprogs failed to build with newer gettext package. This was due to a problem in auto-fu. This patch fixes this allowing the packages to build correctly.

BZ#675694

If more than 128 devices were specified on the blkid command line, the devices[] array overflowed, resulting in a crash. This patch avoids the problem by dynamically allocating the devices[] array based on the number of arguments, resulting in more than 128 devices being able to be specified on the blkid command line.

BZ#696930

Running blkid on s390x caused a crash with a signal 11 (segmentation fault) error. This was due to an error in the code regarding floating points. This patch frees a pointer that was not initialized to null, allowing blkid to run correctly on s390x.

BZ#678304

It was possible for the UUIDD to generate duplicate UIDs under certain circumstances. This occurred when the socket backlog in the UUIDD daemon was full, therefore the connection was refused and uuid_generate_time() fell back to unsafe ways of generating a UUID, resulting in the duplicates. Also, fcntle(2) did not work for the synchronization of threads belonging to the same process, contributing to the problem. This patch introduces a safe variant of uuid_generate_time() and fixes the locking of the clock state counter file which prevents UUIDD from generating duplicate UIDs.

BZ#681071

Running e2fsck on a corrupted file system gave a “should never happen” error. This occurred when a directory with an htree index had an incorrect and too-large i_size field. This patch prevents e2fsck from crashing and prompts the user to remove the htree index so that it can be rebuilt after pass 3, allowing file systems with this error to be fixed.

Enhancements:

BZ#563909

When running blkid, stale mounts can occasionally be seen within the cache. While running blkid -c /dev/null gets around this, it can become a runtime issue when blkid is run against a machine with several hundred disks. As such this patch adds a garbage collection routine feature. This performs a garbage collection pass on the /etc/blkid.tab file by adding the -g option to the blkid program. The man page has also been updated with more information about what the -g garbage collection option does.

BZ#587778

The mkfs reserved blocks were originally set to 5% by default, with a 1% step size. This was considered excessive for large file systems. With this patch, the reserved blocks amount now accepts a floating point for better accuracy when setting the percent. Also, mke2fs and tune2fs now accept a floating point number from the user to improve the level of accuracy offered.

All users are advised to upgrade to these updated packages, which resolve these issues and include these features.

1.32. EMACS

1.32.1. RHBA-2011:0468: emacs bug fix update

Updated emacs packages that fix various bugs are now available for Red Hat Enterprise Linux 5.

GNU Emacs is a powerful, customizable, self-documenting text editor. It provides special code editing features, a scripting language (elisp), and the capability to read email and news.

This update fixes the following bugs:

* Previously, the emacs and emacs-nox packages did not provide any convenient way for other packages to specify a dependency that can be satisfied by either of the emacs variants. This update changes the emacs and emacs-nox packages and provides the common symbol "emacs(bin)". (BZ#466580)

* Previously, the emacs-nox program was compiled with variable argument function calls, which caused the program to terminate because it violated stack protection boundaries. This occurred, for example, when the user tried to kill a buffer with modifications. This update changes the emacs-nox package to call the variable argument functions without triggering the stack protection. This update also enables the stack protection for the emacs package. (BZ#499035)

All users of emacs are advised to upgrade to these updated packages, which fix these bugs.

1.33. ETHERBOOT

1.33.1. RHBA-2011:0982: etherboot bug fix update

Updated etherboot packages that fix two bugs are now available for Red Hat Enterprise Linux 5.

Etherboot is an open source network bootloader. It provides a direct replacement for proprietary Preboot eXecution Environment (PXE) ROMs. It also has many extra features, such as DNS, HTTP and iSCSI.

This update fixes the following bugs:

* Prior to this update, the debuginfo in etherboot was empty. This update drops the debuginfo package. Now, etherboot contains no more redundant subpackages. (BZ#500578)

* Prior to this update, etherboot could loop forever if a valid PXE offer was not received. Due to this problem, the Virtual Machine (VM) could become unresponsive indefinitely. With this update, etherboot transfers in such cases the control back to the basic input/output system (BIOS) of the VM. Now, the VM can boot from the configured boot method. (BZ#655266)

All etherboot users are advised to upgrade to these updated packages, which fix these bugs.

1.34. EXIM

1.34.1. RHSA-2011:0153: Moderate exim security update

Updated exim packages that fix one security issue are now available for Red Hat Enterprise Linux 4 and 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.

Exim is a mail transport agent (MTA) developed at the University of Cambridge for use on UNIX systems connected to the Internet.

A privilege escalation flaw was discovered in Exim. If an attacker were able to gain access to the "exim" user, they could cause Exim to execute arbitrary commands as the root user. (CVE-2010-4345)

This update adds a new configuration file, "/etc/exim/trusted-configs". To prevent Exim from running arbitrary commands as root, Exim will now drop privileges when run with a configuration file not listed as trusted. This could break backwards compatibility with some Exim configurations, as the trusted-configs file only trusts "/etc/exim/exim.conf" and "/etc/exim/exim4.conf" by default. If you are using a configuration file not listed in the new trusted-configs file, you will need to add it manually.

Additionally, Exim will no longer allow a user to execute exim as root with the -D command line option to override macro definitions. All macro definitions that require root permissions must now reside in a trusted configuration file.

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

1.34.2. RHBA-2011:0443: exim bug fix update

Updated exim packages that fix two bugs are now available for Red Hat Enterprise Linux 5.

Exim is a message transfer agent (MTA) developed at the University of Cambridge for use on UNIX systems connected to the Internet. It provides a flexible solution with extensive facilities for checking incoming mail, and can be installed in place of Sendmail.

This update fixes the following bugs:

* Due to an error in the spec file, dynamic loading of the local_scan() function was not enabled. This update resolves this issue, and dynamic loading of local_scan() is now supported as expected. (BZ#567309)

* Prior to this update, some of the Exim tools were installed without a corresponding manual page. This error has been fixed, and all binaries are now installed with a manual page. (BZ#612466)

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

1.35. FINGER

1.35.1. RHBA-2011:0467: finger bug fix update

Updated finger packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The finger utility allows users to display information about the system users, including their login names, full names, and the time they logged in to the system.

The update fixes the following bug:

* When the finger utility is run with no additional command line options, it provides output in the form of a table. Prior to this update, this tabular output did not include a separate column for information about a host, and this information was incorrectly displayed in the "Office" column. This update adds a new column named "Host", so that the host information no longer appears in the wrong column. (BZ#563291)

All users of finger are advised to upgrade to these updated packages, which fix this bug.

1.36. FIREFOX

1.36.1. RHSA-2011:0885: Critical firefox security and bug fix update

Updated firefox packages that fix several security issues and one bug are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having critical 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.

Mozilla Firefox is an open source web browser. XULRunner provides the XUL Runtime environment for Mozilla Firefox.

A flaw was found in the way Firefox handled malformed JPEG images. A website containing a malicious JPEG image could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox. (CVE-2011-2377)

Multiple dangling pointer flaws were found in Firefox. 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-2011-0083, CVE-2011-0085, CVE-2011-2363)

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-2011-2364, CVE-2011-2365, CVE-2011-2374, CVE-2011-2375, CVE-2011-2376)

An integer overflow flaw was found in the way Firefox handled JavaScript Array objects. A website containing malicious JavaScript could cause Firefox to execute that JavaScript with the privileges of the user running Firefox. (CVE-2011-2371)

A use-after-free flaw was found in the way Firefox handled malformed JavaScript. A website containing malicious JavaScript could cause Firefox to execute that JavaScript with the privileges of the user running Firefox. (CVE-2011-2373)

It was found that Firefox could treat two separate cookies as interchangeable if both were for the same domain name but one of those domain names had a trailing "." character. This violates the same-origin policy and could possibly lead to data being leaked to the wrong domain. (CVE-2011-2362)

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 3.6.18. You can find a link to the Mozilla advisories in the References section of this erratum.

This update also fixes the following bug:

* With previous versions of Firefox on Red Hat Enterprise Linux 5, the "background-repeat" CSS (Cascading Style Sheets) property did not work (such images were not displayed and repeated as expected). (BZ#698313)

All Firefox users should upgrade to these updated packages, which contain Firefox version 3.6.18, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

1.36.2. RHSA-2011:0471: Critical firefox security update

Updated firefox packages that fix several security issues are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having critical 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.

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 possibly lead to arbitrary code execution with the privileges of the user running Firefox. (CVE-2011-0080, CVE-2011-0081)

An arbitrary memory write flaw was found in the way Firefox handled out-of-memory conditions. If all memory was consumed when a user visited a malicious web page, it could possibly lead to arbitrary code execution with the privileges of the user running Firefox. (CVE-2011-0078)

An integer overflow flaw was found in the way Firefox handled the HTML frameset tag. A web page with a frameset tag containing large values for the "rows" and "cols" attributes could trigger this flaw, possibly leading to arbitrary code execution with the privileges of the user running Firefox. (CVE-2011-0077)

A flaw was found in the way Firefox handled the HTML iframe tag. A web page with an iframe tag containing a specially-crafted source address could trigger this flaw, possibly leading to arbitrary code execution with the privileges of the user running Firefox. (CVE-2011-0075)

A flaw was found in the way Firefox displayed multiple marquee elements. A malformed HTML document could cause Firefox to execute arbitrary code with the privileges of the user running Firefox. (CVE-2011-0074)

A flaw was found in the way Firefox handled the nsTreeSelection element. Malformed content could cause Firefox to execute arbitrary code with the privileges of the user running Firefox. (CVE-2011-0073)

A use-after-free flaw was found in the way Firefox appended frame and iframe elements to a DOM tree when the NoScript add-on was enabled. Malicious HTML content could cause Firefox to execute arbitrary code with the privileges of the user running Firefox. (CVE-2011-0072)

A directory traversal flaw was found in the Firefox resource:// protocol handler. Malicious content could cause Firefox to access arbitrary files accessible to the user running Firefox. (CVE-2011-0071)

A double free flaw was found in the way Firefox handled "application/http-index-format" documents. A malformed HTTP response could cause Firefox to execute arbitrary code with the privileges of the user running Firefox. (CVE-2011-0070)

A flaw was found in the way Firefox handled certain JavaScript cross-domain requests. If malicious content generated a large number of cross-domain JavaScript requests, it could cause Firefox to execute arbitrary code with the privileges of the user running Firefox. (CVE-2011-0069)

A flaw was found in the way Firefox displayed the autocomplete pop-up. Malicious content could use this flaw to steal form history information. (CVE-2011-0067)

Two use-after-free flaws were found in the Firefox mObserverList and mChannel objects. Malicious content could use these flaws to execute arbitrary code with the privileges of the user running Firefox. (CVE-2011-0066, CVE-2011-0065)

A flaw was found in the Firefox XSLT generate-id() function. This function returned the memory address of an object in memory, which could possibly be used by attackers to bypass address randomization protections. (CVE-2011-1202)

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 3.6.17. You can find a link to the Mozilla advisories in the References section of this erratum.

All Firefox users should upgrade to these updated packages, which contain Firefox version 3.6.17, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

1.36.3. RHSA-2011:0373: Important firefox security update

Updated firefox packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having important security impact.

Mozilla Firefox is an open source web browser. XULRunner provides the XUL Runtime environment for Mozilla Firefox.

This erratum blacklists a small number of HTTPS certificates. (BZ#689430)

All Firefox users should upgrade to these updated packages, which contain a backported patch. After installing the update, Firefox must be restarted for the changes to take effect.

1.36.4. RHSA-2011:0310: Critical firefox security and bug fix update

Updated firefox packages that fix several security issues and one bug are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having critical 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.

Mozilla Firefox is an open source web browser. XULRunner provides the XUL Runtime environment for Mozilla Firefox.

A flaw was found in the way Firefox sanitized HTML content in extensions. If an extension loaded or rendered malicious content using the ParanoidFragmentSink class, it could fail to safely display the content, causing Firefox to execute arbitrary JavaScript with the privileges of the user running Firefox. (CVE-2010-1585)

A flaw was found in the way Firefox handled dialog boxes. An attacker could use this flaw to create a malicious web page that would present a blank dialog box that has non-functioning buttons. If a user

closes the dialog box window, it could unexpectedly grant the malicious web page elevated privileges. (CVE-2011-0051)

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-2011-0053, CVE-2011-0055, CVE-2011-0058, CVE-2011-0062)

Several flaws were found in the way Firefox handled malformed JavaScript. A website containing malicious JavaScript could cause Firefox to execute that JavaScript with the privileges of the user running Firefox. (CVE-2011-0054, CVE-2011-0056, CVE-2011-0057)

A flaw was found in the way Firefox handled malformed JPEG images. A website containing a malicious JPEG image could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox. (CVE-2011-0061)

A flaw was found in the way Firefox handled plug-ins that perform HTTP requests. If a plug-in performed an HTTP request, and the server sent a 307 redirect response, the plug-in was not notified, and the HTTP request was forwarded. The forwarded request could contain custom headers, which could result in a Cross Site Request Forgery attack. (CVE-2011-0059)

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 3.6.14. You can find a link to the Mozilla advisories in the References section of this erratum.

This update also fixes the following bug:

* On Red Hat Enterprise Linux 4 and 5, running the "firefox -setDefaultBrowser" command caused warnings such as the following:

libgnomevfs-WARNING **: Deprecated function. User modifications to the MIME database are no longer supported.

This update disables the "setDefaultBrowser" option. Red Hat Enterprise Linux 4 users wishing to set a default web browser can use Applications -> Preferences -> More Preferences -> Preferred Applications. Red Hat Enterprise Linux 5 users can use System -> Preferences -> Preferred Applications. (BZ#463131, BZ#665031)

All Firefox users should upgrade to these updated packages, which contain Firefox version 3.6.14, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

1.37. FLASH-PLUGIN

1.37.1. RHSA-2011:0869: Critical flash-plugin security update

An updated Adobe Flash Player package that fixes one security issue is now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

The Red Hat Security Response Team has rated this update as having critical 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 flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

This update fixes one vulnerability in Adobe Flash Player. This vulnerability is detailed on the Adobe security page APSB11-18, listed in the References section. Specially-crafted SWF content could cause flash-plugin to crash or, potentially, execute arbitrary code. (CVE-2011-2110)

All users of Adobe Flash Player should install this updated package, which upgrades Flash Player to version 10.3.181.26.

1.37.2. RHSA-2011:0850: Important flash-plugin security update

An updated Adobe Flash Player package that fixes one security issue is now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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 flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

This update fixes one vulnerability in Adobe Flash Player. This vulnerability is detailed on the Adobe security page APSB11-13, listed in the References section. (CVE-2011-2107)

All users of Adobe Flash Player should install this updated package, which upgrades Flash Player to version 10.3.181.22

1.37.3. RHSA-2011:0511: Critical flash-plugin security update

An updated Adobe Flash Player package that fixes multiple security issues is now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

The Red Hat Security Response Team has rated this update as having critical 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 flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

This update fixes multiple vulnerabilities in Adobe Flash Player. These vulnerabilities are detailed on the Adobe security page APSB11-12, listed in the References section.

Multiple security flaws were found in the way flash-plugin displayed certain SWF content. An attacker could use these flaws to create a specially-crafted SWF file that would cause flash-plugin to crash or, potentially, execute arbitrary code when the victim loaded a page containing the specially-crafted SWF content. (CVE-2011-0618, CVE-2011-0619, CVE-2011-0620, CVE-2011-0621, CVE-2011-0622, CVE-2011-0623, CVE-2011-0624, CVE-2011-0625, CVE-2011-0626, CVE-2011-0627)

This update also fixes an information disclosure flaw in flash-plugin. (CVE-2011-0579)

All users of Adobe Flash Player should install this updated package, which upgrades Flash Player to version 10.3.181.14.

1.37.4. RHSA-2011:0451: Critical flash-plugin security update

An updated Adobe Flash Player package that fixes one security issue is now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

The Red Hat Security Response Team has rated this update as having critical 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 flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

This update fixes one vulnerability in Adobe Flash Player. This vulnerability is detailed on the Adobe security page APSB11-07, listed in the References section. Specially-crafted SWF content could cause flash-plugin to crash or, potentially, execute arbitrary code. (CVE-2011-0611)

All users of Adobe Flash Player should install this updated package, which upgrades Flash Player to version 10.2.159.1.

1.37.5. RHSA-2011:0372: Critical flash-plugin security update

An updated Adobe Flash Player package that fixes one security issue is now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

The Red Hat Security Response Team has rated this update as having critical 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 flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

This update fixes one vulnerability in Adobe Flash Player. This vulnerability is detailed on the Adobe security page APSB11-05, listed in the References section. Specially-crafted SWF content could cause flash-plugin to crash or, potentially, execute arbitrary code. (CVE-2011-0609)

All users of Adobe Flash Player should install this updated package, which upgrades Flash Player to version 10.2.153.1.

1.37.6. RHSA-2011:0206: Critical flash-plugin security update

An updated Adobe Flash Player package that fixes multiple security issues is now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

The Red Hat Security Response Team has rated this update as having critical 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 flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

This update fixes multiple vulnerabilities in Adobe Flash Player. These vulnerabilities are detailed on the Adobe security page APSB11-02, listed in the References section.

Multiple security flaws were found in the way flash-plugin displayed certain SWF content. An attacker could use these flaws to create a specially-crafted SWF file that would cause flash-plugin to crash or, potentially, execute arbitrary code when the victim loaded a page containing the specially-crafted SWF content. (CVE-2011-0558, CVE-2011-0559, CVE-2011-0560, CVE-2011-0561, CVE-2011-0571, CVE-2011-0572, CVE-2011-0573, CVE-2011-0574, CVE-2011-0575, CVE-2011-0577, CVE-2011-0578, CVE-2011-0607, CVE-2011-0608)

All users of Adobe Flash Player should install this updated package, which upgrades Flash Player to version 10.2.152.27.

1.38. FONTS-INDIC

1.38.1. RHEA-2011:0978: fonts-indic enhancement update

An updated fonts-indic package which adds a glyph for the new Indian Rupee Sign is now available for Red Hat Enterprise Linux 5.

The fonts-indic package provides a free Indian Script TrueType and OpenType font.

This update adds the following enhancement:

* Unicode 6.0, the most recent major version of the Unicode standard, was released 2011-10-11. Among 2,088 new characters added to the standard is the Indian Rupee Sign, the new official Indian currency symbol. With this update, the fonts-indic package now includes a glypo for this new character, U+20B9. (BZ#674486)

All users requiring the Indian rupee sign should install this updated package, which adds this enhancement.

1.39. GCC

1.39.1. RHBA-2011:1029: gcc bug fix update

Updated gcc packages that fix three bugs are now available for Red Hat Enterprise Linux 5.

The gcc packages provide compilers for C, C++, Java, Fortran, Objective C, and Ada 95 GNU, as well as related support libraries.

This update fixes the following bugs:

* Prior to this update, aliasing problems could occur when the wrong value type was used for reading the vtable. Due to these problems, the pointer-to-member handling in the C++ frontend could cause miscompilations. This update accesses the correct value type. (BZ#630893)

* Prior to this update, the debug information wrongly indicated that a variable with Named Return Value (NRV) was located in a certain register when only its address was located in the register. With this update, the source code is modified so that the debug information contains the correct information. (BZ#660302)

* Prior to this update, gcc-c++ produced redundant duplicate entries in the dwarf debug information for class variables with virtual functions. This update modifies the code so that class variables are entered only once. (BZ#660305)

All GCC users are advised to upgrade to these updated packages, which fix these bugs.

1.40. GDB

1.40.1. RHBA-2011:1024: gdb bug fix update

An updated gdb package that fixes various bugs is now available for Red Hat Enterprise Linux 5.

The GNU Debugger, GDB, allows the debugging of programs written in C, C++, and other languages by executing them in a controlled fashion and printing the debug data.

This updated gdb package includes fixes for the following bugs:

* Previously, a change to the list of shared libraries could have corrupted the internal "bpstat" structure. Consequent to this, typing the "info program" command at a GDB prompt could have caused the utility to terminate unexpectedly with a segmentation fault. This update ensures that the "bpstat" structure always contains the correct data, and running the "info program" command no longer causes the debugger to terminate unexpectedly. (BZ#660197)

* A multithreaded program can be dumped into a core file. GDB can load the core file and display the list of its threads. Previously, GDB displayed for the threads found in the core file only their LWP (light-weight process) identifiers, which match the Linux TID (Thread Identifier) values. With this update, GDB initializes the libthread_db threads debugging library when accessing a core file and now displays the pthread_t identifier in addition to the LWP identifier. (BZ#673697)

* The Fortran programming language is case-insensitive. When compiling Fortran programs with the Intel Fortran Compiler, the compiler records some debug info symbols in uppercase. The gfortran compiler writes case-insensitive symbols in lowercase. Because of this, GDB could have terminated unexpectedly while accessing uppercase characters in the debug information from the Intel Fortran Compiler. With this update, GDB properly implements case insensitivity and ignores the symbols case in the symbol files. (BZ#645773)

* GDB crashed when reading a kernel core dump file because the value of the temporary current inferior process was set to minus_one_ptid (all processes). The value is now set to null_ptid (no processes) and GDB displays the vmcore file correctly. (BZ#696464)

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

1.40.2. RHBA-2011:0186: gdb bug fix update

An updated gdb package that fixes a bug is now available for Red Hat Enterprise Linux 5.

The GNU Debugger, GDB, allows the debugging of programs written in C, C++, and other languages by executing them in a controlled fashion and then printing out their data.

This update fixes the following bug:

* Previously, a change to the list of shared libraries could corrupt the internal "bpstat" structure. Consequent to this, typing the "info program" command at a GDB prompt could cause the utility to terminate unexpectedly with a segmentation fault. This update ensures that the "bpstat" structure always contains the correct data, and running the "info program" command no longer causes the debugger to crash. (BZ#669636)

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

1.41. GDBM

1.41.1. RHBA-2011:0172: gdbm bug fix update

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

The gdbm package is a GNU database indexing library, including routines which use extensible hashing.

This updated gdbm package fixes the following bug:

* Prior to this update, some applications performed poorly while using the "dbm_*" calls to perform operations on database files hosted on a NFS share. This was caused by thousands of flock calls made by the "gdbm_*" calls which in turn were called by the "dbm_*()" functions used in applications. These flock calls are inefficient when used over a NFS share since they result in a call being made over the wire and result in the cache on the NFS client being invalidated. This update adds a new environment variable "NDBM_LOCK". The "dbm_open" function now reads the "NDBM_LOCK" environment variable and if this variable is set to false ("NDBM_LOCK=false/no/off/0"), the "dbm_open" function does not lock the database. (BZ#668689)

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

1.42. GFS-UTILS

1.42.1. RHBA-2011:1041: gfs-utils bug fix update

An updated gfs-utils package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The gfs-utils package provides various user-space tools necessary to mount, create, maintain, and test Global File Systems (GFS).

This update fixes the following bug:

* Prior to this update, the performance of the gfs_fsck utility was very slow. This update modifies the source code to improve the GFS check utility (gfs_fsck). The performance gain depends on the contents of the file system and the amount of corruption encountered. (BZ#515834)

All users of gfs-utils are advised to upgrade to this updated package, which resolves this bug.

1.43. GFS2-UTILS

1.43.1. RHBA-2011:1042: gfs2-utils bug fix and enhancement update

Updated gfs2-utils packages that fix multiple bugs and add one enhancement are now available for Red Hat Enterprise Linux 5.

The gfs2-utils packages provide the user-space utilities necessary to mount, create, maintain and test GFS2 file systems.

This update fixes the following bugs:

* Prior to this update, gfs2_grow aborted unexpectedly with an error message on a full file system If no free blocks were available in the file system, and the last block of the rindex file did not allow to add more resource group entries. As a workaround, the user must remove or truncate a file to free up space. Once the file system is grown, the file can safely be added back. (BZ# 490649)

* Prior to this update, a file system check (fsck) on GFS2 file systems in verbose mode caused misleading error messages that the master and root inodes were not correctly marked. This update modifies the code to set both the master and root inodes as "in use" in the in-core block map. Now, fsck.gfs2 realizes that the master and root inodes are properly marked. (BZ# 642797)

* Prior to this update, a fsck on a GFS2 file system for i686 calculated the wrong starting point for its bitmap search because the GFS2 bitmap was in the wrong state. Due to this issue, the bitmap search

was stuck in an infinite loop. This update modifies the calculation to use the correct size on 32-bit platforms. Now, the fsck.gfs2 check runs as expected. (BZ# 667769)

* Prior to this update, a file system check on a damaged GFS2 file system containing two inodes that point to the same metadata appeared to be a "duplicate block reference" but both were unrecoverable. Due to this issue, the fsck.gfs2 check in pass1b terminated abnormally with a segmentation fault because of the empty reference list. This update additionally checks whether the duplicate reference list is empty. Now, pass1b completes normally and fsck.gfs2 finishes as expected. (BZ#679076)

* Prior to this update, the command "gfs2_edit savemeta" did not save all directory information for large directories. Due to this behavior, the directory hash table and directory leaf blocks beneath were not saved. This update modifies the savemeta function for gfs2_edit to read all the data. With the directory hash table processed correctly, all leaf blocks are saved as expected. (BZ# 679565)

* Prior to this update, indirect blocks were prematurely released from a gfs2_edit savemeta queue. Due to this behavior, some meta data was not saved and consequently meta data sets restored with gfs2_edit restoremeta did not pass a file system check (fsck). This update modifies gfs2_edit so that the required blocks are now left on the queue and saved with the rest of the meta data. Now, saving the meta data of a consistent file system results in a complete meta data set which passes a fsck when restored. (BZ# 698298)

This update also adds the following enhancement:

* Prior to this update, gfs2_edit gathered GFS2 file system information less effectively. This update enhances gfs_edit to gather more information. (BZ# 656371)

All gfs2-utils users are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

1.43.2. RHBA-2011:0476: gfs2-utils bug fix update

An updated gfs2-utils package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The gfs2-utils package provides the user-space tools necessary to mount, create, maintain, and test GFS2 file systems.

This update fixes the following bug:

* On 32-bit x86 architectures, an attempt to check a large GFS2 file system caused the fsck.gfs2 utility to enter an infinite loop, utilizing 100% of available CPU resources. When run with the "-vv" option, the fsck.gfs2 command would produce output similar to the following:

(pass1.c:1453) Already processed system inode 33121 (0x8161)

This update applies an upstream patch that prevents such infinite loop, and large GFS2 file systems now successfully complete their file system check on both 32-bit and 64-bit architectures. (BZ#675911)

All users of gfs2-utils are advised to upgrade to this updated package, which fixes this bug.

1.44. GIFLIB

1.44.1. RHBA-2011:0398: giflib bug fix update

Updated giflib packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The giflib packages contain a shared library of functions for loading and saving GIF image files. This library is API and ABI compatible with libungif, the library that supported uncompressed GIF image files while the Unisys LZW patent was in effect.

This update fixes the following bug:

* Prior to this update, an attempt to use the giftext utility on a GIF file that does not store a global color map caused it to terminate unexpectedly with a segmentation fault. This update applies an upstream patch that resolves this issue, and giftext no longer crashes. (BZ#249555)

All users of giflib are advised to upgrade to these updated packages, which fix this bug.

1.45. GIMP

1.45.1. RHSA-2011:0838: Moderate gimp security update

Updated gimp packages that fix multiple security issues 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 GIMP (GNU Image Manipulation Program) is an image composition and editing program.

An integer overflow flaw, leading to a heap-based buffer overflow, was found in the GIMP's Microsoft Windows Bitmap (BMP) and Personal Computer eXchange (PCX) image file plug-ins. An attacker could create a specially-crafted BMP or PCX image file that, when opened, could cause the relevant plug-in to crash or, potentially, execute arbitrary code with the privileges of the user running the GIMP. (CVE-2009-1570, CVE-2011-1178)

A heap-based buffer overflow flaw was found in the GIMP's Paint Shop Pro (PSP) image file plug-in. An attacker could create a specially-crafted PSP image file that, when opened, could cause the PSP plug-in to crash or, potentially, execute arbitrary code with the privileges of the user running the GIMP. (CVE-2010-4543)

A stack-based buffer overflow flaw was found in the GIMP's Lightning, Sphere Designer, and Gfig image filters. An attacker could create a specially-crafted Lightning, Sphere Designer, or Gfig filter configuration file that, when opened, could cause the relevant plug-in to crash or, potentially, execute arbitrary code with the privileges of the user running the GIMP. (CVE-2010-4540, CVE-2010-4541, CVE-2010-4542)

Red Hat would like to thank Stefan Cornelius of Secunia Research for responsibly reporting the CVE-2009-1570 flaw.

Users of the GIMP are advised to upgrade to these updated packages, which contain backported patches to correct these issues. The GIMP must be restarted for the update to take effect.

1.46. GLIBC

1.46.1. RHSA-2011:0412: Important glibc security update

Updated glibc packages that fix multiple 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.

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, a Linux system cannot function properly.

The fix for CVE-2010-3847 introduced a regression in the way the dynamic loader expanded the $ORIGIN dynamic string token specified in the RPATH and RUNPATH entries in the ELF library header. A local attacker could use this flaw to escalate their privileges via a setuid or setgid program using such a library. (CVE-2011-0536)

It was discovered that the glibc addmntent() function did not sanitize its input properly. A local attacker could possibly use this flaw to inject malformed lines into /etc/mtab via certain setuid mount helpers, if the attacker were allowed to mount to an arbitrary directory under their control. (CVE-2010-0296)

It was discovered that the glibc fnmatch() function did not properly restrict the use of alloca(). If the function was called on sufficiently large inputs, it could cause an application using fnmatch() to crash or, possibly, execute arbitrary code with the privileges of the application. (CVE-2011-1071)

It was discovered that the locale command did not produce properly escaped output as required by the POSIX specification. If an attacker were able to set the locale environment variables in the environment of a script that performed shell evaluation on the output of the locale command, and that script were run with different privileges than the attacker's, it could execute arbitrary code with the privileges of the script. (CVE-2011-1095)

All users should upgrade to these updated packages, which contain backported patches to correct these issues.

1.46.2. RHBA-2011:1034: glibc bug fix update

Updated glibc packages that fix multiple bugs are now available for Red Hat Enterprise Linux 5.

The glibc packages provide the standard C and standard math libraries used by multiple programs on the system. Without these libraries, the Linux system cannot function correctly.

This update fixes the following bugs:

* Prior to this update, SELinux stopped the worker module on 64-bit architectures, which prevented servers from loading. This was caused by the executable stack not being allocated when the first 4 GB of the address space were exhausted. This modifies the code so that servers now load correctly. (BZ#448011)

* Prior to this update, the dynamic loader generated an incorrect ordering for initialization according to the ELF specification. Initialization routines for depended-upon objects were not being called before the objects, which depended on them, were initialized. This manifested itself only when initializing compiled C++ libraries whose global initialization depended upon the global initialization of data in other libraries which were linked against at link time, generating a DT_NEEDED entry. This update modifies the topological sort algorithm for dependency resolution. Now, functions for initialization and termination are ordered correctly. (BZ#604796)

* Prior to this update, the expansion of the "$ORIGIN" dynamic string token in "RPATH" elements for privileged programs was disabled. Due to this problem, certain libraries such as gconv did not work correctly. This update re-enables this feature for libraries. Now, the libraries work as expected. (BZ#670988)

* Prior to this update, the resolver failed to return all addresses of multi-homed hosts in /etc/hosts. Now, getaddrinfo correctly initializes the resolver state on the first call. (BZ#676039)

* Prior to this update, the PHTREAD_CANCEL_DISABLE could, under certain conditions, fail to prevent thread cancellations. Due to this problem, pthread_cancel could cancel input/output (I/O) like write and read calls while PTHREAD_CANCEL_DISABLE was in effect. With this update, the cancellations work as expected. (BZ#684808)

* Prior to this update, the glibc libraries could fail to allocate enough memory for the expanded strings when expanding the dynamic string tokens in load paths for the dynamic linker or in module names for the "dlopen" function. Due to this behavior, certain applications could freeze or terminate unexpectedly with an error message. This update modifies the underlying source code to allocate enough memory for the expanded strings. (BZ#694655)

All users of glibc are advised to upgrade to these updated packages, which fix these bugs.

1.46.3. RHBA-2011:0466: glibc bug fix update

Updated glibc packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The glibc packages provide the standard C and standard math libraries used by multiple programs on the system. Without these libraries, the Linux system cannot function properly.

This update fixes the following bug:

* When expanding the dynamic string tokens in load paths for the dynamic linker or in module names for the "dlopen" function, previous versions of the glibc libraries may have failed to allocate enough memory for the expanded strings, causing certain applications to terminate unexpectedly with the following error:

malloc(): memory corruption: 0x09b43fd0

With this update, the underlying source code has been adapted to allocate enough memory for the expanded strings, and the glibc libraries no longer cause applications to crash. (BZ#695258)

All users are advised to upgrade to these updated packages, which fix this bug.

1.46.4. RHBA-2011:0901: glibc bug fix update

Updated glibc packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The glibc packages provide the standard C and standard math libraries used by multiple programs on the system. Without these libraries, the Linux system cannot function properly.

This update fixes the following bug:

* Previously, the dynamic loader generated an incorrect ordering for initialization according to the ELF specification. Initialization routines for depended-upon objects were not being called before the objects, which depended on them, were being initialized. This manifested itself only when initializing compiled C++ libraries whose global initialization depended upon the global initialization of data in other libraries which they were linked against at link time, generating a DT_NEEDED entry. With this update, implementation of the topological sort algorithm for dependency resolution has been fixed, and functions for initialization and termination are now ordered correctly. (BZ#711778)

All users are advised to upgrade to these updated packages, which fix this bug.

1.47. GNOME-SCREENSAVER

1.47.1. RHBA-2011:0286: gnome-screensaver bug fix update

An updated gnome-screensaver package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The gnome-screensaver package contains the GNOME project's official screen saver program. It is designed for improved integration with a GNOME desktop, including themeability, language support, and Human Interface Guidelines (HIG) compliance. It also provides screen-locking and fast user-switching from a locked screen.

This update fixes the following bug:

* Previously, using the "Pictures folder" screen saver with an empty Pictures directory could cause the gnome-screensaver program to terminate unexpectedly. This update applies an upstream patch that resolves this issue, and an empty Pictures directory no longer causes the "Pictures folder" screen saver to crash. (BZ#673990)

All users of gnome-screensaver are advised to upgrade to this updated package, which resolves this issue.

1.48. GNOME-TERMINAL

1.48.1. RHBA-2011:1082: gnome-terminal bug fix update

An updated gnome-terminal package that fixes a bug is now available for Red Hat Enterprise Linux 5.

Gnome-terminal is a terminal emulator for GNOME. It supports translucent backgrounds, opening multiple terminals in a single window (tabs) and clickable URLs.

This updated gnome-terminal package fixes the following enhancement:

* When the HTTP_PROXY environment variable was set with the ignore_hosts option in the GConf configuration system, this setting was not honored in terminal applications. With this update, the code has been modified to better honor GNOME proxy configuration in terminal applications. (BZ#719399)

All users of gnome-terminal are advised to upgrade to this updated package, which fixes this bug.

1.49. GNOME-VFS2

1.49.1. RHBA-2011:0441: gnome-vfs2 bug fix update

Updated gnome-vfs2 packages that fix two bugs are now available for Red Hat Enterprise Linux 5.

The gnome-vfs2 packages provide the GNOME virtual file system (GNOME VFS) which is the foundation of the Nautilus file manager.

This update fixes the following bugs:

* Previously, the ImageMagick tool set closed unexpectedly with a segmentation fault after successful conversion during exit due to an incompatibility with the atexit handler when unloading librsvg. This update uses __attribute__((destructor)) instead of atexit(). Now, ImageMagick no longer closes unexpectedly after successful conversion. (BZ#472253)

* When using the GNOME desktop with an ext4 file system, moving a file located on the ext4 file system did not result in the file being correctly moved to the Trash. This update corrects the VFS code so that moving files to the Trash succeeds as expected on ext4 file systems. (BZ#594836)

All gnome-vfs2 users are advised to upgrade to these updated packages, which fix these bugs.

1.50. GZIP

1.50.1. RHBA-2011:0976: gzip bug fix update

An updated gzip package that fixes two bugs is now available for Red Hat Enterprise Linux 5.

The gzip package provides the GNU gzip data compression program.

This update fixes the following bugs:

* Previously, an automatic attempt to close the standard output (stdout) stream could under certain circumstances fail. However, the gzip utility did not check if the final stdout close was successful. Due to this issue, the gzip utility could cause silent data loss while it returned a zero exit status, indicating success. This update closes the stdin and stdout streams carefully at exit time. Now, a non-zero exit status is returned if there are any problems while closing the stdin or stdout streams. (BZ#514562)

* Previously, the gzip(1) man page contained a typographic error. This update corrects this error. Now, the manual page is typographically correct. (BZ#675464)

Users of gzip are advised to upgrade to this updated package, which fixes these bugs.

1.51. HPLIP

1.51.1. RHSA-2011:0154: Moderate hplip security update

Updated hplip packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

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.

Hewlett-Packard Linux Imaging and Printing (HPLIP) provides drivers for Hewlett-Packard printers and multifunction peripherals, and tools for installing, using, and configuring them.

A flaw was found in the way certain HPLIP tools discovered devices using the SNMP protocol. If a user ran certain HPLIP tools that search for supported devices using SNMP, and a malicious user is able to send specially-crafted SNMP responses, it could cause those HPLIP tools to crash or, possibly, execute arbitrary code with the privileges of the user running them. (CVE-2010-4267)

Red Hat would like to thank Sebastian Krahmer of the SuSE Security Team for reporting this issue.

Users of hplip should upgrade to these updated packages, which contain a backported patch to correct this issue.

1.52. HTTPD

1.52.1. RHBA-2011:1067: httpd bug fix and enhancement update

Updated httpd packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

IMPORTANT

This update was released as errata RHBA-2011:1067 — httpd bug fix and enhancement update.

The Apache HTTP Server is a popular web server.

Bug Fixes:

BZ#264681

Prior to this update, using any **mod_ldap** directive within a **`VirtualHost`** context prevented the module from caching results for that particular virtual host. This update adapts the **mod_ldap** module to make sure that caching now works correctly in such configurations.

BZ#552303, BZ#632407

When the **mod_proxy** module was configured as a reverse proxy, multiple unrelated bugs may have prevented it from operating correctly, and may have led to incorrect handling of connection timeouts or even data corruption. With this update, various patches have been applied to address this issue, and the **mod_proxy** module can now serve as a reverse proxy as expected.

BZ#580008

When the **mod_deflate** module was configured to compress responses and an HTTP client prematurely terminated a connection, the previous version of the **`httpd`** service may have terminated unexpectedly with a segmentation fault. This update applies a patch that resolves this issue, and **`httpd`** no longer crashes.

BZ#604727

Prior to this update, the **mod_authnz_ldap** module was unable to handle referrals from an LDAP server. This update introduces the **`LDAPChaseReferrals`** directive, which allows users to enable referral chasing.

BZ#614423

Previously, when the **`OID`**() function was used as part of the **`SSLRequire`** directive, it was unable to parse certificate attributes of an unknown type. Consequent to this, strings that use the Abstract Syntax Notation One (ASN.1) notation were not rendered properly, and may have been incorrectly prefixed with a random string. This update adapts the **`OID`**() function to parse all unknown attributes as ASN.1 strings, so that these strings are now rendered as expected.

BZ#649648

Due to incorrect handling of the SSL certificate cache, an attempt to use an SSL configuration with multiple **`VirtualHost`** sections that use identical **`ServerName`** values rendered the **`httpd`** service unable to start. With this update, the underlying source code has been adapted to address this issue, and using multiple **`VirtualHost`** sections with identical **`ServerNames`** values no longer prevents **`httpd`** from starting.

BZ#673276

Due to incorrect handling of responses with multiple duplicate headers, when a user configured the **httpd** service to transform HTTP response headers by specifying `edit` as a value of the `Header` directive, only one of the matching headers was retained. This has now been fixed, and the `edit` mode is now applied correctly across all HTTP response headers.

BZ#674102

When using the **prefork** Multi-Processing Module (MPM), children processes with persistent connections (that is, with the `KeepAlive` directive set to `On`) kept processing new requests even when a graceful restart had been issued. This update applies a patch that corrects this error, and children processes with persistent connections no longer process new requests when a graceful restart is requested.

BZ#678057

Prior to this update, an attempt to use the `ProxyPassReverse` directive with a `balancer://` URL that included a path segment caused redirect responses to map the HTTP Location header paths incorrectly. This error has been fixed, and HTTP Location header paths are now mapped correctly.

BZ#679994

Previously, the `FilterProvider` directive of the `mod_filter` module was unable to match against non-standard HTTP response headers. With this update, the underlying source code has been adapted to address this issue, and the `FilterProvider` directive is now able to match against non-standard HTTP response headers as expected.

BZ#691497

When configured as a reverse proxy, the previous version of the **mod_proxy** module was unable to establish an SSL connection via an intermediary proxy configured using the `ProxyRemote` directive. This update adapts the **mod_proxy** module to support this configuration.

BZ#698402

Prior to this update, the **mod_include** module may have failed to parse certain Server Side Include (SSI) documents if the response contained attribute boundaries that were split across multiple buckets. This update corrects this error, and such SSI documents can now be parsed as expected.

Enhancements:

BZ#379811

When using the **mod_cache** module, by default, the `CacheMaxExpire` directive is only applied to responses which do not specify their expiry date. Previously, it was not possible to limit the maximum expiry time for all resources. This update adapts the **mod_cache** module to provide support for `hard` as a second argument of the `CacheMaxExpire` directive, allowing a maximum expiry time to be enforced for all resources.

BZ#555870

The **mod_proxy_balancer** load balancer module has been updated to provide support for the *bybusyness* scheduler algorithm.

BZ#612198

The **mod_reqtimeout** module has been added. When enabled, this module allows fine-grained timeouts to be applied during request parsing.

BZ#658766

The **mod_proxy** and **mod_proxy_http** modules have been updated to provide support for remote HTTPS proxy servers by using the **HTTP CONNECT** method.

All users of httpd are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

1.52.2. RHBA-2011:0480: httpd bug fix update

Updated httpd packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The Apache HTTP Server is a popular web server.

This update fixes the following bug:

* When the mod_proxy module was configured as a reverse proxy using HTTP over SSL/TLS to a back-end server, data from the back end could be incorrectly truncated. This update applies a backported patch that resolves this issue, and using a reverse proxy with HTTP over SSL/TLS no longer causes the Apache HTTP Server to serve corrupted data. (BZ#694158)

All users of httpd are advised to upgrade to these updated packages, which fix this bug.

1.53. HWDATA

1.53.1. RHEA-2011:1011: hwdata enhancement update

An updated hwdata package that adds various enhancements is now available for Red Hat Enterprise Linux 5.

The hwdata package contains tools for accessing and displaying hardware identification and configuration data.

This update adds the following enhancements:

* This update introduces support for the IMMv2 management controller and the integrated Matrox MGA-G200ER graphics chipset. (BZ#592427)

* This update enables hardware support for upcoming Intel products releases. (BZ#571823)

* The pci.ids database has been updated according to the latest upstream changes. (BZ#677671)

All users of hwdata are advised to upgrade to this updated package, which adds these enhancements.

1.54. IA32EL

1.54.1. RHBA-2011:1037: ia32el bug fix update

An updated ia32el package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The ia32el package contains the IA-32 Execution Layer platform, which allows emulation of IA-32 binaries on Intel Itanium processors.

This updated package fixes the following bug:

* Prior to this update, a well-formed multi-threaded program aborted unexpectedly with a segmentation fault or a double free abort due to a conflict between malloc and free library calls. With this update, the code is modified so that a well-formed program runs as expected. (BZ#548655)

All users of ia32el are advised to upgrade to this updated package which resolves this bug.

1.55. INITSCRIPTS

1.55.1. RHBA-2011:1081: initscripts bug fix and enhancement update

An updated initscripts package that fixes various bugs and add several enhancements is now available for Red Hat Enterprise Linux 5.

IMPORTANT

This update was released as errata RHBA-2011:1081 — initscripts bug fix and enhancement update.

The initscripts package contains system scripts to boot your system, change runlevels, activate and deactivate most network interfaces, and shut the system down cleanly.

Bug Fixes:

BZ#699544

After system installation, the **dhclient** utility failed to start after boot on an interface configured to get an IPv4 address from DHCP. This bug has been fixed and the **dhclient** utility now starts properly in the described scenario.

BZ#624704

Previously, when a logical network with VLAN tag 0 was created, this value was out of range for logical networks, the host would never create a sub interface 0 and the cluster network would stay in non-operational mode. With this update, the **/etc/sysconfig/network-scripts/ifup** script has been fixed and logical networks with VLAN tag 0 can now be created.

BZ#676851

Previously, when the **netfs** script performed a lazy unmount on a NFS file system, sometimes cached data would be written out before the shutdown scripts were able to take down the network interfaces. This caused various machines to have been hanging on shutdown. With this update, the **netfs** script has been fixed and the physical machines no longer hang in the described scenario.

BZ#664091

When the **biosdevname** utility sets a name for a PCI device, it uses a # character to specify the device interface. Subsequently, when network services were restarted, the **network** init script returned an error message, such as `ifcfg-ifcfg-pci3#1: No such file or directory` even though the interface itself was properly found. With this update, the **network** init script parses the # character correctly and no error messages are given in the described scenario.

BZ#462095

If an Ethernet interface had letters in the device file name (such as `ethWAN` or `ethVZ`) instead of just numbers (such as `eth0` or `eth5`), the **/sbin/ifup** script failed to enable VLANs configured on such interfaces after the network service was restarted. This bug has been fixed and the **/sbin/ifup**

script now properly configures VLANs regardless of their names.

BZ#604669

When a bonding interface was configured in the **/etc/modprobe.conf** file without specifying the options in the **BONDING_OPTS** variable, the ***arp_ip_target*** parameter value was cleared after a network restart. Subsequently, the interface connection could not be restored. With this update, the **ifdown-eth** script has been fixed to only add the ***arp_ip_target*** parameter if it is not present, fixing this bug.

BZ#649995

Previously, the following diagnostic error message was given in every **tcsh** shell:

```
grep: character class syntax is [[:space:]], not [:space:].
```

This bug has been fixed in the **/etc/profile.d/lang.csh** script and the error message is no longer returned.

BZ#671386

Due to a change in a status message of the **dmraid** utility, the following error messages appeared on boot, when the previous version of the initscripts package was installed:

```
failed to stat() /dev/mapper/no
failed to stat() /dev/mapper/block
failed to stat() /dev/mapper/devices
failed to stat() /dev/mapper/found
```

With this update, the **/rc.d/rc.sysinit** script has been fixed and the error messages no longer appear on boot.

BZ#685038

When a system was rebooted while the network switch was down and the network interface had the **PERSISTENT_DHCLIENT** variable set to **yes**, the **dhclient** utility still failed to start on boot. With this update, the **ifup-eth** init script has been fixed and the **dhclient** utility starts as expected when **PERSISTENT_DHCLIENT=yes** is configured.

BZ#687849

Previously, when no Internet Small Computer System Interface (iSCSI) check was done during shutdown or reboot, the following redundant error message was given:

```
find: /sys/class/iscsi_session/: No such file or directory.
```

With this update, the **/etc/rc.d/init.d/network** script has been fixed and the error message is no longer displayed.

BZ#687890

Previously, the following redundant error message was given during system shutdown:

```
Unmounting file systems:  Cannot umount ""
```

With this update, the **/rc.d/init.d/functions** script has been fixed and the error message is no longer displayed.

BZ#692893

Due to a bug in the **/etc/ssh/ssh_config** init script, the value of the **LANG** variable overwrote the same variable on a remote system as the config settings were passed via OpenSSH, even if the **LANG** variable was already set. This sometimes caused undesired locale settings with unsupported character set to be set on the target system. This bug has been fixed and the **LANG** variable is no longer overwritten in the described scenario.

BZ#703203

Due to a bug in the **/etc/init.d/halt** script, no mount point set up with the word **nfs** anywhere in its path could be unmounted at reboot or shutdown. This bug has been fixed and such mount points are now unmounted properly.

BZ#684909

Previously, if no IPv4 address was configured, then DHCP for an IPv6 address was not carried out. Subsequently, the eth0 interface had the default IPv6 link-local address assigned to it, instead the address that would be allocated to it via IPv6 **dhcpd** utility. This bug has been fixed in the **/etc/sysconfig/network-scripts/ifup-eth** script and now, the **dhcp6c** daemon is started and an IPv6 address is acquired for the address as well as additional information such as DNS servers etc.

BZ#674221

Previously, if a bonded interface was created and the slave interface includes the setting **MASTER=bond0** (where **bond0** is the bonded interface) the slave did not start. This bug has been fixed in the **/etc/sysconfig/network-scripts/ifcfg-ethX** script and the bonded interface now brings up the slave interface and communicate as expected.

BZ#669728

Previously, when MAC (Media Access Control) addresses were switched on a virtual machine or a physical machine with two network interfaces, the **sbin/ifdown** script became unresponsive when the network was restarted. With this update, the script recognizes that the MAC address for the network interface is wrong and then ignores it, thus fixing this bug.

BZ#665601

The **sysctl** utility uses **.** as the path delimiter while VLAN interfaces use **.** as the ID delimiter. This conflict caused all **sysctl** calls on a VLAN interface to terminate without any output, causing various issues with IPv6 auto-configuration feature. With this update, several scripts of the iniscripts package have been patched and the **sysctl** calls no longer hang on VLAN interfaces.

BZ#648524

Previously, the **/sysconfig/network-scripts/network-functions** script calculated wrong value of the **DEVICETYPE** variable for IPoIB (IP over Infiniband) child interfaces. Subsequently, the variable could not be used to handle the specific need of the interface, such as calling the **ifup-${DEVICETYPE}** script. This bug has been fixed and the **DEVICETYPE** variable value is now calculated correctly for IPoIB interfaces.

BZ#637176

When multiple PIDs (Process Identifiers) are passed to the **checkpid()** function, it exits with the return value of **0** after finding the first existing PID. This is intended behavior of the function but the

accompanying comment in the code indicated that the function fully supported multiple PIDs as arguments, which was confusing for some users. With this update, the comment in the code has been clarified.

BZ#713988

When the X Window System was started by the `startx` command on the console, the desktop was always displayed in English regardless of the language configured in the `/etc/sysconfig/i18n` file. With this update, the bug has been fixed in the **/etc/profile.d/lang.sh** script, and the language setting is now properly recognized when X starts.

Enhancements:

BZ#624385

With this update, various init scripts have been enhanced so that they are able to parse configuration files located in the `/etc/sysctl.d/` directory. This makes it easier to install or remove RPM packages packages that modify kernel runtime parameters.

BZ#612877

With this update, the **ifup** and **ifdown** scripts can recognize and act upon configuration for IPv6 that contains alias devices. Now, multiple IPv6 addresses can be configured on the same interface and can be controlled separately.

BZ#507515

With this update, the **ifup** script reports duplicate IP addresses via the **syslog** utility to the `/var/log/messages` file, in addition to printing its messages on standard output.

BZ#653621

With this update, support for the 1731/02 OSM/OSX network device has been added to the initscrips package.

BZ#689898

With this update, an explanatory comment has been added to the **/rc.d/init.d/netfs** and the **/rc.d/rc.sysinit** init scripts regarding the `mount -t no*` syntax.

All users of initscript are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

1.56. IPA-CLIENT

1.56.1. RHBA-2011:0990: ipa-client bug fix update

An updated ipa-client package that fixes two bugs is now available for Red Hat Enterprise Linux 5.

The ipa-client package provides a tool to enroll a machine to an IPA version 2 server. IPA (Identity, Policy, Audit) is an integrated solution to provide centrally managed identity, that is, machine, user, virtual machines, groups, and authentication credentials.

This update fixes the following bug:

* This update adds sssd suport to the ipa-client package. (BZ#631907)

* Previously, the ipa-client used the wrong object identifier (OID). This update corrects this issue. Now, the ipa-client uses the same OID as the the server. (BZ #682231)

All IPA users are advised to upgrade to this updated package which, fixes this bug.

1.56.2. RHBA-2011:0832: ipa-client bug fix update

An updated ipa-client package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The ipa-client package provides a tool to enroll a machine to an IPA version 2 server. IPA (Identity, Policy, Audit) is an integrated solution to provide centrally managed identity, that is, machine, user, virtual machines, groups, and authentication credentials.

This update fixes the following bug:

* Previously, the ipa-client used the wrong object identifier (OID). This update corrects this issue. Now, the ipa-client uses the same OID as the server (BZ #704649)

All IPA users are advised to upgrade to this updated package which, fixes this bug.

1.57. IPRUTILS

1.57.1. RHEA-2011:0992: iprutils enhancement update

An updated iprutils package that provides one enhancement is now available for Red Hat Enterprise Linux 5.

The iprutils package provides utilities to manage and configure SCSI devices that are supported by the ipr SCSI storage device driver.

This update adds the following enhancement:

* The iprutils package has been updated to provide support for the Serial Attached SCSI (SAS) vRAID functions. (BZ#651439)

All users of iprutils are advised to upgrade to this updated iprutils package, which adds this enhancement.

1.58. IPVSADM

1.58.1. RHBA-2011:0979: ipvsadm bug fix update

An updated ipvsadm package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The ipvsadm package provides the ipsvadm tool to administer the IP Virtual Server services offered by the Linux kernel.

This update fixes the following bug:

* Prior to this update, the kernel module ipvs was automatically loaded if the ipvsadm module was not loaded when checking the ipvsadm service status. This behavior affected the system configuration, especially the memory usage. This update ensures that the ipvsadm service status check does not load the kernel module on systems without the loaded ipsvadm module. (BZ#592264)

All users of ipvsadm are advised to upgrade to this updated package, which fixes this bug.

1.59. ISCSI-INITIATOR-UTILS

1.59.1. RHBA-2011:1033: iscsi-initiator-utils bug fix and enhancement update

An updated iscsi-initiator-utils package that fixes two bugs and adds various enhancements is now available for Red Hat Enterprise Linux 5.

The iscsi-initiator-utils package provides the 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 (IP) networks.

This update fixes the following bugs:

* Prior to this update, the iscsid service and Broadcom iSCSI driver's user space component were not synchronized when logging into an iSCSI target. As a result, the iSCSI login timeout could have been reached or a login error could have been issued under certain circumstances. The bug has been fixed in this update so that iscsid and the user space component are now synchronized and the iSCSI login process works as expected. (BZ#595549)

* Prior to this update, trying to establish a connection to an iSCSI target using the bnx2i offload interface transport could have failed due to the iSCSI daemon and bnx2i driver not being in sync during initialization. Furthermore, any number of machine restarts had no effect on this undesired behavior. The bug has been fixed in this update so that the connection with bnx2i can now be successfully established as expected. (BZ#572596)

As well, this update adds the following enhancements:

* Broadcom iSCSI driver's user space component has been upgraded to upstream version 0.6.2.14, which adds support for the Broadcom 57712 10Gb controller, IPv6 networking, virtual LAN support, and subnet masking. (BZ#660434)

* With this update, the iscsi-initiator-utils package now supports the Chelsio T4 iSCSI offload cards using the cxgb4i driver. (BZ#640121)

* With this update, the iscsi-initiator-utils package is now built for the IBM System z platform. (BZ#567852)

All users of iscsi-initiator-utils should upgrade to this updated package, which fixes these bugs and adds these enhancements.

1.60. IWL6000-FIRMWARE

1.60.1. RHEA-2011:0971: iwl6000-firmware bug fix and enhancement update

An updated iwl6000-firmware package that fixes several bugs, adds various enhancements, and matches the iwlagn driver in the latest Red Hat Enterprise Linux 6 kernels, is now available.

The iwlagn driver requires firmware loaded on the device in order to function. This package provides the firmware required by that driver for Intel Wireless WiFi Link 6000 series adapters.

The iwl6000-firmware package has been upgraded to upstream version 9.221.4.1, which provides a number of bug fixes and enhancements over the previous version. (BZ#568033)

Users of the iwlagn driver are advised to upgrade to this updated iwl6000-firmware package, which resolves these issues and adds these enhancements.

1.61. JABBERD

1.61.1. RHSA-2011:0882: Low Red Hat Network Satellite server jabberd security update

An updated jabberd package that fixes one security issue is now available for Red Hat Network Satellite 5.4.1 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.

This package provides jabberd 2, an Extensible Messaging and Presence Protocol (XMPP) server used for XML based communication.

It was found that the jabberd daemon did not properly detect recursion during entity expansion. A remote attacker could provide a specially-crafted XML file containing a large number of nested entity references, which once processed by the jabberd daemon, could lead to a denial of service (excessive memory and CPU consumption). (CVE-2011-1755)

Red Hat would like to thank Nico Golde of the Debian Security Team for reporting this issue. The Debian Security Team acknowledges Wouter Coekaerts as the original reporter.

Users of Red Hat Network Satellite 5.4.1 are advised to upgrade to this updated jabberd package, which resolves this issue. For this update to take effect, Red Hat Network Satellite must be restarted. Refer to the Solution section for details.

1.61.2. RHSA-2011:0881: Low Red Hat Network Proxy server jabberd security update

An updated jabberd package that fixes one security issue is now available for Red Hat Network Proxy 5.4.1 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.

This package provides jabberd 2, an Extensible Messaging and Presence Protocol (XMPP) server used for XML based communication.

It was found that the jabberd daemon did not properly detect recursion during entity expansion. A remote attacker could provide a specially-crafted XML file containing a large number of nested entity references, which once processed by the jabberd daemon, could lead to a denial of service (excessive memory and CPU consumption). (CVE-2011-1755)

Red Hat would like to thank Nico Golde of the Debian Security Team for reporting this issue. The Debian Security Team acknowledges Wouter Coekaerts as the original reporter.

Users of Red Hat Network Proxy 5.4.1 are advised to upgrade to this updated jabberd package, which resolves this issue. For this update to take effect, Red Hat Network Proxy must be restarted. Refer to the Solution section for details.

1.62. JAVA-1.4.2-IBM

1.62.1. RHSA-2011:0490: Critical java-1.4.2-ibm security update

Updated java-1.4.2-ibm packages that fix several security issues are now available for Red Hat Enterprise Linux 4 Extras and Red Hat Enterprise Linux 5 Supplementary.

The Red Hat Security Response Team has rated this update as having critical 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 IBM 1.4.2 SR13-FP9 Java release includes the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit.

This update fixes several vulnerabilities in the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit. Detailed vulnerability descriptions are linked from the IBM "Security alerts" page, listed in the References section. (CVE-2010-4447, CVE-2010-4448, CVE-2010-4454, CVE-2010-4462, CVE-2010-4465, CVE-2010-4466, CVE-2010-4473, CVE-2010-4475, CVE-2011-0311)

All users of java-1.4.2-ibm are advised to upgrade to these updated packages, which contain the IBM 1.4.2 SR13-FP9 Java release. All running instances of IBM Java must be restarted for this update to take effect.

1.62.2. RHSA-2011:0292: Moderate java-1.4.2-ibm security update

Updated java-1.4.2-ibm packages that fix one security issue are now available for Red Hat Enterprise Linux 4 Extras and Red Hat Enterprise Linux 5 Supplementary.

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 IBM 1.4.2 SR13-FP8 Java release includes the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit.

A denial of service flaw was found in the way certain strings were converted to Double objects. A remote attacker could use this flaw to cause Java based applications to hang, for example, if they parsed Double values in a specially-crafted HTTP request. (CVE-2010-4476)

All users of java-1.4.2-ibm are advised to upgrade to these updated packages, which contain the IBM 1.4.2 SR13-FP8 Java release. All running instances of IBM Java must be restarted for this update to take effect.

1.62.3. RHSA-2011:0152: Moderate java-1.4.2-ibm security update

Updated java-1.4.2-ibm packages that fix two security issues are now available for Red Hat Enterprise Linux 4 Extras and Red Hat Enterprise Linux 5 Supplementary.

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 IBM 1.4.2 SR13-FP8 Java release includes the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit.

This update fixes two vulnerabilities in the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit. Detailed vulnerability descriptions are linked from the IBM "Security alerts" page, listed in the References section. (CVE-2010-1321, CVE-2010-3574)

Note: The RHSA-2010:0935 java-1.4.2-ibm update did not, unlike the erratum text stated, provide fixes for the above issues.

All users of java-1.4.2-ibm are advised to upgrade to these updated packages, which contain the IBM 1.4.2 SR13-FP8 Java release. All running instances of IBM Java must be restarted for this update to take effect.

1.63. JAVA-1.4.2-IBM-SAP

1.63.1. RHSA-2011:0870: Moderate java-1.4.2-ibm-sap security update

Updated java-1.4.2-ibm-sap packages that fix several security issues are now available for Red Hat Enterprise Linux 4, 5 and 6 for SAP.

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 IBM 1.4.2 SR13-FP9 Java release includes the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit.

This update fixes several vulnerabilities in the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit. Detailed vulnerability descriptions are linked from the IBM "Security alerts" page, listed in the References section. (CVE-2010-4447, CVE-2010-4448, CVE-2010-4454, CVE-2010-4462, CVE-2010-4465, CVE-2010-4466, CVE-2010-4473, CVE-2010-4475, CVE-2011-0311)

All users of java-1.4.2-ibm-sap for Red Hat Enterprise Linux 4, 5 and 6 for SAP are advised to upgrade to these updated packages, which contain the IBM 1.4.2 SR13-FP9 Java release. All running instances of IBM Java must be restarted for this update to take effect.

1.63.2. RHSA-2011:0299: Moderate java-1.4.2-ibm-sap security update

Updated java-1.4.2-ibm-sap packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5 and 6 for SAP.

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 IBM 1.4.2 SR13-FP8 Java release includes the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit.

A denial of service flaw was found in the way certain strings were converted to Double objects. A remote attacker could use this flaw to cause Java based applications to hang, for example, if they parsed Double values in a specially-crafted HTTP request. (CVE-2010-4476)

Note: The java-1.4.2-ibm packages were renamed to java-1.4.2-ibm-sap to correct a naming overlap; however, java-1.4.2-ibm-sap does not automatically obsolete the previous java-1.4.2-ibm packages for Red Hat Enterprise Linux 4 and 5 for SAP. Refer to the RHBA-2010:0491 and RHBA-2010:0530 advisories, listed in the References, for further information.

All users of java-1.4.2-ibm-sap for Red Hat Enterprise Linux 4, 5 and 6 for SAP are advised to upgrade to these updated packages, which contain the IBM 1.4.2 SR13-FP8 Java release. All running instances of IBM Java must be restarted for this update to take effect.

1.64. JAVA-1.5.0-IBM

1.64.1. RHSA-2011:0364: Critical java-1.5.0-ibm security update

Updated java-1.5.0-ibm packages that fix several security issues are now available for Red Hat Enterprise Linux 4 Extras, and Red Hat Enterprise Linux 5 and 6 Supplementary.

The Red Hat Security Response Team has rated this update as having critical 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 IBM 1.5.0 Java release includes the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit.

This update fixes several vulnerabilities in the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit. Detailed vulnerability descriptions are linked from the IBM "Security alerts" page, listed in the References section. (CVE-2010-4447, CVE-2010-4448, CVE-2010-4450, CVE-2010-4454, CVE-2010-4462, CVE-2010-4465, CVE-2010-4466, CVE-2010-4468, CVE-2010-4471, CVE-2010-4473, CVE-2010-4475)

All users of java-1.5.0-ibm are advised to upgrade to these updated packages, containing the IBM 1.5.0 SR12-FP4 Java release. All running instances of IBM Java must be restarted for this update to take effect.

1.64.2. RHSA-2011:0291: Moderate java-1.5.0-ibm security update

Updated java-1.5.0-ibm packages that fix one security issue are now available for Red Hat Enterprise Linux 4 Extras, and Red Hat Enterprise Linux 5 and 6 Supplementary.

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 IBM 1.5.0 Java release includes the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit.

A denial of service flaw was found in the way certain strings were converted to Double objects. A remote attacker could use this flaw to cause Java based applications to hang, for example, if they parsed Double values in a specially-crafted HTTP request. (CVE-2010-4476)

All users of java-1.5.0-ibm are advised to upgrade to these updated packages, containing the IBM 1.5.0 SR12-FP3 Java release. All running instances of IBM Java must be restarted for this update to take effect.

1.64.3. RHSA-2011:0169: Critical java-1.5.0-ibm security and bug fix update

Updated java-1.5.0-ibm packages that fix multiple security issues and one bug are now available for Red Hat Enterprise Linux 4 Extras, and Red Hat Enterprise Linux 5 and 6 Supplementary.

The Red Hat Security Response Team has rated this update as having critical 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 IBM 1.5.0 Java release includes the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit.

This update fixes multiple vulnerabilities in the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit. Detailed vulnerability descriptions are linked from the IBM "Security alerts" page, listed in the References section. (CVE-2010-3553, CVE-2010-3557, CVE-2010-3571)

This update also fixes the following bug:

* An error in the java-1.5.0-ibm RPM spec file caused an incorrect path to be included in HtmlConverter, preventing it from running. (BZ#659710)

All users of java-1.5.0-ibm are advised to upgrade to these updated packages, containing the IBM 1.5.0 SR12-FP3 Java release. All running instances of IBM Java must be restarted for this update to take effect.

1.65. JAVA-1.6.0-IBM

1.65.1. RHSA-2011:0938: Critical java-1.6.0-ibm security update

Updated java-1.6.0-ibm packages that fix several security issues are now available for Red Hat Enterprise Linux 4 Extras, and Red Hat Enterprise Linux 5 and 6 Supplementary.

The Red Hat Security Response Team has rated this update as having critical 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 IBM 1.6.0 Java release includes the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit.

This update fixes several vulnerabilities in the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit. Detailed vulnerability descriptions are linked from the IBM "Security alerts" page, listed in the References section. (CVE-2011-0802, CVE-2011-0814, CVE-2011-0862, CVE-2011-0863, CVE-2011-0865, CVE-2011-0867, CVE-2011-0868, CVE-2011-0869, CVE-2011-0871, CVE-2011-0873)

All users of java-1.6.0-ibm are advised to upgrade to these updated packages, containing the IBM 1.6.0 SR9-FP2 Java release. All running instances of IBM Java must be restarted for the update to take effect.

1.65.2. RHSA-2011:0357: Critical java-1.6.0-ibm security update

Updated java-1.6.0-ibm packages that fix several security issues are now available for Red Hat Enterprise Linux 4 Extras, and Red Hat Enterprise Linux 5 and 6 Supplementary.

The Red Hat Security Response Team has rated this update as having critical 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 IBM 1.6.0 Java release includes the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit.

This update fixes several vulnerabilities in the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit. Detailed vulnerability descriptions are linked from the IBM "Security alerts" page, listed in the References section. (CVE-2010-4422, CVE-2010-4447, CVE-2010-4448, CVE-2010-4452, CVE-2010-4454, CVE-2010-4462, CVE-2010-4463, CVE-2010-4465, CVE-2010-4466, CVE-2010-4467, CVE-2010-4468, CVE-2010-4471, CVE-2010-4473, CVE-2010-4475)

Note: The RHSA-2010:0987 and RHSA-2011:0290 java-1.6.0-ibm errata were missing 64-bit PowerPC packages for Red Hat Enterprise Linux 4 Extras. This erratum provides 64-bit PowerPC packages for Red Hat Enterprise Linux 4 Extras as expected.

All users of java-1.6.0-ibm are advised to upgrade to these updated packages, containing the IBM 1.6.0 SR9-FP1 Java release. All running instances of IBM Java must be restarted for the update to take effect.

1.65.3. RHSA-2011:0290: Moderate java-1.6.0-ibm security update

Updated java-1.6.0-ibm packages that fix one security issue are now available for Red Hat Enterprise Linux 4 Extras, and Red Hat Enterprise Linux 5 and 6 Supplementary.

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 IBM 1.6.0 Java release includes the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit.

A denial of service flaw was found in the way certain strings were converted to Double objects. A remote attacker could use this flaw to cause Java based applications to hang, for example, if they parsed Double values in a specially-crafted HTTP request. (CVE-2010-4476)

All users of java-1.6.0-ibm are advised to upgrade to these updated packages, containing the IBM 1.6.0 SR9 Java release. All running instances of IBM Java must be restarted for the update to take effect.

1.65.4. RHSA-2011:0880: Low Red Hat Network Satellite server IBM Java Runtime security update

Updated java-1.6.0-ibm packages that fix several security issues are now available for Red Hat Network Satellite 5.4.1 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.

This update corrects several security vulnerabilities in the IBM Java Runtime Environment shipped as part of Red Hat Network Satellite 5.4.1. In a typical operating environment, these are of low security risk as the runtime is not used on untrusted applets.

This update fixes several vulnerabilities in the IBM Java 2 Runtime Environment. Detailed vulnerability descriptions are linked from the IBM "Security alerts" page, listed in the References section. (CVE-2009-3555, CVE-2010-1321, CVE-2010-3541, CVE-2010-3548, CVE-2010-3549, CVE-2010-3550, CVE-2010-3551, CVE-2010-3553, CVE-2010-3555, CVE-2010-3556, CVE-2010-3557, CVE-2010-3558, CVE-2010-3560, CVE-2010-3562, CVE-2010-3563, CVE-2010-3565, CVE-2010-3566, CVE-2010-3568, CVE-2010-3569, CVE-2010-3571, CVE-2010-3572, CVE-2010-3573, CVE-2010-3574, CVE-2010-4422, CVE-2010-4447, CVE-2010-4448, CVE-2010-4452, CVE-2010-4454, CVE-2010-4462, CVE-2010-4463, CVE-2010-4465, CVE-2010-4466, CVE-2010-4467, CVE-2010-4468, CVE-2010-4471, CVE-2010-4473, CVE-2010-4475, CVE-2010-4476)

Users of Red Hat Network Satellite 5.4.1 are advised to upgrade to these updated java-1.6.0-ibm packages, which contain the IBM 1.6.0 SR9-FP1 Java release. For this update to take effect, Red Hat Network Satellite must be restarted. Refer to the Solution section for details.

1.66. JAVA-1.6.0-OPENJDK

1.66.1. RHSA-2011:0857: Important java-1.6.0-openjdk security update

Updated java-1.6.0-openjdk 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.

These packages provide the OpenJDK 6 Java Runtime Environment and the OpenJDK 6 Software Development Kit.

Integer overflow flaws were found in the way Java2D parsed JPEG images and user-supplied fonts. An attacker could use these flaws to execute arbitrary code with the privileges of the user running an untrusted applet or application. (CVE-2011-0862)

It was found that the MediaTracker implementation created Component instances with unnecessary access privileges. A remote attacker could use this flaw to elevate their privileges by utilizing an untrusted applet or application that uses Swing. (CVE-2011-0871)

A flaw was found in the HotSpot component in OpenJDK. Certain bytecode instructions confused the memory management within the Java Virtual Machine (JVM), resulting in an applet or application crashing. (CVE-2011-0864)

An information leak flaw was found in the NetworkInterface class. An untrusted applet or application could use this flaw to access information about available network interfaces that should only be available to privileged code. (CVE-2011-0867)

An incorrect float-to-long conversion, leading to an overflow, was found in the way certain objects (such as images and text) were transformed in Java2D. A remote attacker could use this flaw to crash an untrusted applet or application that uses Java2D. (CVE-2011-0868)

It was found that untrusted applets and applications could misuse a SOAP connection to incorrectly set global HTTP proxy settings instead of setting them in a local scope. This flaw could be used to intercept HTTP requests. (CVE-2011-0869)

A flaw was found in the way signed objects were deserialized. If trusted and untrusted code were running in the same Java Virtual Machine (JVM), and both were deserializing the same signed object, the untrusted code could modify said object by using this flaw to bypass the validation checks on signed objects. (CVE-2011-0865)

Note: All of the above flaws can only be remotely triggered in OpenJDK by calling the "appletviewer" application.

All users of java-1.6.0-openjdk are advised to upgrade to these updated packages, which provide OpenJDK 6 b20 / IcedTea 1.9.8 and resolve these issues. All running instances of OpenJDK Java must be restarted for the update to take effect.

1.66.2. RHSA-2011:0281: Important java-1.6.0-openjdk security update

Updated java-1.6.0-openjdk packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6.

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.

These packages provide the OpenJDK 6 Java Runtime Environment and the OpenJDK 6 Software Development Kit.

A flaw was found in the Swing library. Forged TimerEvents could be used to bypass SecurityManager checks, allowing access to otherwise blocked files and directories. (CVE-2010-4465)

A flaw was found in the HotSpot component in OpenJDK. Certain bytecode instructions confused the memory management within the Java Virtual Machine (JVM), which could lead to heap corruption. (CVE-2010-4469)

A flaw was found in the way JAXP (Java API for XML Processing) components were handled, allowing them to be manipulated by untrusted applets. This could be used to elevate privileges and bypass secure XML processing restrictions. (CVE-2010-4470)

It was found that untrusted applets could create and place cache entries in the name resolution cache. This could allow an attacker targeted manipulation over name resolution until the OpenJDK VM is restarted. (CVE-2010-4448)

It was found that the Java launcher provided by OpenJDK did not check the LD_LIBRARY_PATH environment variable for insecure empty path elements. A local attacker able to trick a user into running the Java launcher while working from an attacker-writable directory could use this flaw to load an untrusted library, subverting the Java security model. (CVE-2010-4450)

A flaw was found in the XML Digital Signature component in OpenJDK. Untrusted code could use this flaw to replace the Java Runtime Environment (JRE) XML Digital Signature Transform or C14N algorithm implementations to intercept digital signature operations. (CVE-2010-4472)

Note: All of the above flaws can only be remotely triggered in OpenJDK by calling the "appletviewer" application.

This update also provides one defense in depth patch. (BZ#676019)

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.

1.66.3. RHSA-2011:0214: Moderate java-1.6.0-openjdk security update

Updated java-1.6.0-openjdk packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

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.

These packages provide the OpenJDK 6 Java Runtime Environment and the OpenJDK 6 Software Development Kit.

A denial of service flaw was found in the way certain strings were converted to Double objects. A remote attacker could use this flaw to cause Java-based applications to hang, for instance if they parse Double values in a specially-crafted HTTP request. (CVE-2010-4476)

All users of java-1.6.0-openjdk are advised to upgrade to these updated packages, which resolve this issue. All running instances of OpenJDK Java must be restarted for the update to take effect.

1.66.4. RHSA-2011:0176: Moderate java-1.6.0-openjdk security update

Updated java-1.6.0-openjdk packages that fix two security issues 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.

These packages provide the OpenJDK 6 Java Runtime Environment and the OpenJDK 6 Software Development Kit. The javaws command can be used to launch Java Web Start applications.

A public static field declaration allowed untrusted JNLP (Java Network Launching Protocol) applications to read privileged data. A remote attacker could directly or indirectly read the values of restricted system properties, such as "user.name", "user.home", and "java.home", which untrusted applications should not be allowed to read. (CVE-2010-3860)

It was found that JNLPSecurityManager could silently return without throwing an exception when permission was denied. If the javaws command was used to launch a Java Web Start application that relies on this exception being thrown, it could result in that application being run with elevated privileges, allowing it to bypass security manager restrictions and gain access to privileged functionality. (CVE-2010-4351)

Note: The RHSA-2010:0339 java-1.6.0-openjdk update installed javaws by mistake. As part of the fixes for CVE-2010-3860 and CVE-2010-4351, this update removes javaws.

Red Hat would like to thank the TippingPoint Zero Day Initiative project for reporting CVE-2010-4351. The original issue reporter wishes to stay anonymous.

This erratum also upgrades the OpenJDK package to IcedTea6 1.7.7. Refer to the NEWS file, linked to in the References, for further information.

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.

1.66.5. RHEA-2011:0485: java-1.6.0-openjdk enhancement update

Enhanced java-1.6.0-openjdk packages are now available for Red Hat Linux 5.

These packages provide the OpenJDK 6 Java Runtime Environment and the OpenJDK 6 Software Development Kit.

These updated java-1.6.0-openjdk packages provide support for the Rhino JavaScript interpreter, an open-source implementation of JavaScript. (BZ#694080)

Note: new rhino and jline packages are also now available separately for Red Hat Enterprise Linux 5. In order to rebuild java-1.6.0-openjdk, you must first install the new rhino and jline packages.

Users of java-1.6.0-openjdk are advised to upgrade to these updated packages, which add this enhancement.

1.67. JAVA-1.6.0-SUN

1.67.1. RHSA-2011:0860: Critical java-1.6.0-sun security update

Updated java-1.6.0-sun packages that fix several security issues are now available for Red Hat Enterprise Linux 4 Extras, and Red Hat Enterprise Linux 5 and 6 Supplementary.

The Red Hat Security Response Team has rated this update as having critical 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 Sun 1.6.0 Java release includes the Sun Java 6 Runtime Environment and the Sun Java 6 Software Development Kit.

This update fixes several vulnerabilities in the Sun Java 6 Runtime Environment and the Sun Java 6 Software Development Kit. Further information about these flaws can be found on the "Oracle Java SE Critical Patch Update Advisory" page, listed in the References section. (CVE-2011-0802, CVE-2011-0814, CVE-2011-0862, CVE-2011-0863, CVE-2011-0864, CVE-2011-0865, CVE-2011-0867, CVE-2011-0868, CVE-2011-0869, CVE-2011-0871, CVE-2011-0873)

All users of java-1.6.0-sun are advised to upgrade to these updated packages, which provide JDK and JRE 6 Update 26 and resolve these issues. All running instances of Sun Java must be restarted for the update to take effect.

1.67.2. RHSA-2011:0282: Critical java-1.6.0-sun security update

Updated java-1.6.0-sun packages that fix several security issues are now available for Red Hat Enterprise Linux 4 Extras, and Red Hat Enterprise Linux 5 and 6 Supplementary.

The Red Hat Security Response Team has rated this update as having critical 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 Sun 1.6.0 Java release includes the Sun Java 6 Runtime Environment and the Sun Java 6 Software Development Kit.

This update fixes several vulnerabilities in the Sun Java 6 Runtime Environment and the Sun Java 6 Software Development Kit. Further information about these flaws can be found on the "Oracle Java SE and Java for Business Critical Patch Update Advisory" page, listed in the References section. (CVE-2010-4422, CVE-2010-4447, CVE-2010-4448, CVE-2010-4450, CVE-2010-4451, CVE-2010-4452, CVE-2010-4454, CVE-2010-4462, CVE-2010-4463, CVE-2010-4465, CVE-2010-4466, CVE-2010-4467, CVE-2010-4468, CVE-2010-4469, CVE-2010-4470, CVE-2010-4471, CVE-2010-4472, CVE-2010-4473, CVE-2010-4475, CVE-2010-4476)

All users of java-1.6.0-sun are advised to upgrade to these updated packages, which resolve these issues. All running instances of Sun Java must be restarted for the update to take effect.

1.68. JBOSS

1.68.1. RHSA-2011:0948: Important JBoss Enterprise Application Platform 5.1.1 update

Updated JBoss Enterprise Application Platform 5.1.1 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 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.

JBoss Enterprise Application Platform is the market-leading platform for innovative and scalable Java applications. JBoss Enterprise Application Platform integrates the JBoss Application Server with JBoss Hibernate and JBoss Seam into a complete and simple enterprise solution.

This JBoss Enterprise Application Platform 5.1.1 release for Red Hat Enterprise Linux 5 serves as a replacement for JBoss Enterprise Application Platform 5.1.0.

These updated packages include the bug fixes detailed in the release notes, which are linked to from the References section of this erratum.

The following security issue is also fixed with this release:

It was found that the fix for CVE-2011-1484 was incomplete: JBoss Seam 2 did not block access to all malicious JBoss Expression Language (EL) constructs in page exception handling, allowing arbitrary Java methods to be executed. A remote attacker could use this flaw to execute arbitrary code via a specially-crafted URL provided to certain applications based on the JBoss Seam 2 framework. Note: A properly configured and enabled Java Security Manager would prevent exploitation of this flaw. (CVE-2011-2196)

Red Hat would like to thank the ObjectWorks+ Development Team at Nomura Research Institute for reporting this issue.

Warning: Before applying this update, please back up your JBoss Enterprise Application Platform's "jboss-as/server/[PROFILE]/deploy/" directory, along with all other customized configuration files.

All users of JBoss Enterprise Application Platform 5.1.0 on Red Hat Enterprise Linux 5 are advised to upgrade to these updated packages. Manual action is required for this update to take effect. Refer to the Solution section for details.

1.68.2. RHSA-2011:0945: Important JBoss Enterprise Web Platform 5.1.1 update

Updated JBoss Enterprise Web Platform 5.1.1 packages that fix one security issue and various bugs are now available for Red Hat Enterprise Linux 4, 5, and 6.

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.

The Enterprise Web Platform is for mid-size workloads, focusing on light and rich Java applications. Web Platform is a slimmed down profile of the JBoss Enterprise Application Platform.

This JBoss Enterprise Web Platform 5.1.1 release for Red Hat Enterprise Linux 4, 5, and 6 serves as a replacement for JBoss Enterprise Web Platform 5.1.0.

These updated packages include the bug fixes detailed in the release notes, which are linked to from the References section of this erratum.

The following security issue is also fixed with this release:

It was found that the fix for CVE-2011-1484 was incomplete: JBoss Seam 2 did not block access to all malicious JBoss Expression Language (EL) constructs in page exception handling, allowing arbitrary Java methods to be executed. A remote attacker could use this flaw to execute arbitrary code via a

specially-crafted URL provided to certain applications based on the JBoss Seam 2 framework. Note: A properly configured and enabled Java Security Manager would prevent exploitation of this flaw. (CVE-2011-2196)

Red Hat would like to thank the ObjectWorks+ Development Team at Nomura Research Institute for reporting this issue.

Warning: Before applying this update, please back up your JBoss Enterprise Web Platform's "jboss-as-web/server/[PROFILE]/deploy/" directory and any other customized configuration files.

All users of JBoss Enterprise Web Platform on Red Hat Enterprise Linux 4, 5, and 6 are advised to upgrade to these updated packages. Manual action is required for this update to take effect. Refer to the Solution section for details.

1.68.3. RHSA-2011:0897: Moderate JBoss Enterprise Web Server 1.0.2 update

JBoss Enterprise Web Server 1.0.2 is now available for Red Hat Enterprise Linux 4, 5, and 6.

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.

JBoss Enterprise Web Server is a fully-integrated and certified set of components for hosting Java web applications.

This is the first release of JBoss Enterprise Web Server for Red Hat Enterprise Linux 6. For Red Hat Enterprise Linux 4 and 5, this release serves as a replacement for JBoss Enterprise Web Server 1.0.1, and includes a number of bug fixes. Refer to the Release Notes, linked in the References, for more information.

This update corrects security flaws in the following components:

tomcat6:

A cross-site scripting (XSS) flaw was found in the Manager application, used for managing web applications on Apache Tomcat. If a remote attacker could trick a user who is logged into the Manager application into visiting a specially-crafted URL, the attacker could perform Manager application tasks with the privileges of the logged in user. (CVE-2010-4172)

tomcat5 and tomcat6:

It was found that web applications could modify the location of the Apache Tomcat host's work directory. As web applications deployed on Tomcat have read and write access to this directory, a malicious web application could use this flaw to trick Tomcat into giving it read and write access to an arbitrary directory on the file system. (CVE-2010-3718)

A second cross-site scripting (XSS) flaw was found in the Manager application. A malicious web application could use this flaw to conduct an XSS attack, leading to arbitrary web script execution with the privileges of victims who are logged into and viewing Manager application web pages. (CVE-2011-0013)

A possible minor information leak was found in the way Apache Tomcat generated HTTP BASIC and DIGEST authentication requests. For configurations where a realm name was not specified and Tomcat was accessed via a proxy, the default generated realm contained the hostname and port used by the proxy to send requests to the Tomcat server. (CVE-2010-1157)

httpd:

A flaw was found in the way the mod_dav module of the Apache HTTP Server handled certain requests. If a remote attacker were to send a carefully crafted request to the server, it could cause the httpd child process to crash. (CVE-2010-1452)

apr:

It was found that the apr_fnmatch() function used an unconstrained recursion when processing patterns with the '*' wildcard. An attacker could use this flaw to cause an application using this function, which also accepted untrusted input as a pattern for matching (such as an httpd server using the mod_autoindex module), to exhaust all stack memory or use an excessive amount of CPU time when performing matching. (CVE-2011-0419)

apr-util:

It was found that certain input could cause the apr-util library to allocate more memory than intended in the apr_brigade_split_line() function. An attacker able to provide input in small chunks to an application using the apr-util library (such as httpd) could possibly use this flaw to trigger high memory consumption. Note: This issue only affected the JBoss Enterprise Web Server packages on Red Hat Enterprise Linux 4. (CVE-2010-1623)

All users of JBoss Enterprise Web Server 1.0.1 are advised to upgrade to JBoss Enterprise Web Server 1.0.2, which corrects these issues. After installing this update, the relevant Apache Tomcat service ("tomcat5" or "tomcat6") and the Apache HTTP Server ("httpd") must be restarted for the update to take effect.

1.69. JBOSS-SEAM2

1.69.1. RHSA-2011:0950: Important jboss-seam2 security update

Updated jboss-seam2 packages that fix one security issue are now available for JBoss Enterprise Application Platform 4.3 for Red Hat Enterprise Linux 4 and 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.

The JBoss Seam 2 framework is an application framework for building web applications in Java.

It was found that the fix for CVE-2011-1484 was incomplete: JBoss Seam 2 did not block access to all malicious JBoss Expression Language (EL) constructs in page exception handling, allowing arbitrary Java methods to be executed. A remote attacker could use this flaw to execute arbitrary code via a specially-crafted URL provided to certain applications based on the JBoss Seam 2 framework. Note: A properly configured and enabled Java Security Manager would prevent exploitation of this flaw. (CVE-2011-2196)

Red Hat would like to thank the ObjectWorks+ Development Team at Nomura Research Institute for reporting this issue.

Users of jboss-seam2 should upgrade to these updated packages, which correct this issue. Manual action is required for this update to take effect. Refer to the Solution section for details.

1.69.2. RHSA-2011:0461: Important jboss-seam2 security update

Updated jboss-seam2 packages that fix one security issue are now available for JBoss Enterprise Application Platform 5.1 for Red Hat Enterprise Linux 4 and 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.

The JBoss Seam 2 framework is an application framework for building web applications in Java.

It was found that JBoss Seam 2 did not properly block access to JBoss Expression Language (EL) constructs in page exception handling, allowing arbitrary Java methods to be executed. A remote attacker could use this flaw to execute arbitrary code via a specially-crafted URL provided to certain applications based on the JBoss Seam 2 framework. Note: A properly configured and enabled Java Security Manager would prevent exploitation of this flaw. (CVE-2011-1484)

Red Hat would like to thank Martin Kouba from IT SYSTEMS a.s. for reporting this issue.

Users of jboss-seam2 should upgrade to these updated packages, which correct this issue. The JBoss server process must be restarted for this update to take effect.

1.69.3. RHSA-2011:0460: Important jboss-seam2 security update

Updated jboss-seam2 packages that fix one security issue are now available for JBoss Enterprise Application Platform 4.3 for Red Hat Enterprise Linux 4 and 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.

The JBoss Seam 2 framework is an application framework for building web applications in Java.

It was found that JBoss Seam 2 did not properly block access to JBoss Expression Language (EL) constructs in page exception handling, allowing arbitrary Java methods to be executed. A remote attacker could use this flaw to execute arbitrary code via a specially-crafted URL provided to certain applications based on the JBoss Seam 2 framework. Note: A properly configured and enabled Java Security Manager would prevent exploitation of this flaw. (CVE-2011-1484)

Red Hat would like to thank Martin Kouba from IT SYSTEMS a.s. for reporting this issue.

Users of jboss-seam2 should upgrade to these updated packages, which correct this issue. The JBoss server process must be restarted for this update to take effect.

1.70. JBOSSWEB

1.70.1. RHSA-2011:0211: Important jbossweb security update

Updated jbossweb packages that fix one security issue are now available for JBoss Enterprise Web Platform 5 for Red Hat Enterprise Linux 4 and 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.

JBoss Web Server is a web container based on Apache Tomcat. It provides a single deployment platform for the JavaServer Pages (JSP) and Java Servlet technologies.

A denial of service flaw was found in the way certain strings were converted to Double objects. A remote attacker could use this flaw to cause JBoss Web Server to hang via a specially-crafted HTTP request. (CVE-2010-4476)

Users of JBoss Web Server should upgrade to these updated packages, which contain a backported patch to correct this issue. The JBoss server process must be restarted for this update to take effect.

1.70.2. RHSA-2011:0210: Important jbossweb security update

Updated jbossweb packages that fix one security issue are now available for JBoss Enterprise Application Platform 4.2, 4.3, and 5.1, for Red Hat Enterprise Linux 4 and 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.

JBoss Web Server is the web container, based on Apache Tomcat, in JBoss Enterprise Application Platform. It provides a single deployment platform for the JavaServer Pages (JSP) and Java Servlet technologies.

A denial of service flaw was found in the way certain strings were converted to Double objects. A remote attacker could use this flaw to cause JBoss Web Server to hang via a specially-crafted HTTP request. (CVE-2010-4476)

Users of JBoss Web Server should upgrade to these updated packages, which contain a backported patch to correct this issue. The JBoss server process must be restarted for this update to take effect.

1.71. JWHOIS

1.71.1. RHEA-2011:0419: jwhois enhancement update

An updated jwhois package that adds one enhancement is now available for Red Hat Enterprise Linux 5.

The jwhois package provides a whois client which is used to obtain information about domain names and IP addresses from whois servers.

This update adds the following enhancement:

* Previously, jwhois did not contain the whois server details for the dotEmarat extension. Due to this issue, whois queries for these extensions were incorrectly directed to whois.internic.net. With this update, the configuration file correctly directs queries for the dotEmarat domains to whois.aeda.net.ae. (BZ#663972)

All users of whois clients are advised to upgrade to this updated package which adds this enhancement.

1.72. KDEBASE

1.72.1. RHBA-2011:0501: kdebase bug fix update

An updated kdebase package that fixes various bugs is now available for Red Hat Enterprise Linux 5.

The K Desktop Environment (KDE) is a graphical desktop environment for the X Window System. The kdebase package includes core applications for the K Desktop Environment.

This update fixes the following bugs:

* Due to incorrect handling of transient groups, closing a dialog box of a Java application could cause the KWin window manager to terminate unexpectedly. This update applies an upstream patch that corrects this error, and KWin no longer crashes when a Java dialog box is closed. (BZ#501483)

* Prior to this update, a race condition in the KWin window manager could cause it to ignore configure requests. Consequent to this, Motif-based applications may have been occasionally displayed with an incorrect window size. With this update, the underlying source code has been adapted to ensure the configure requests are received, and Motif applications are now always displayed with a correct window size. (BZ#561844)

* When a user's password expires, the KDM login manager displays a dialog box that forces the user to change the password upon the next login. Previously, canceling this dialog box caused KDM to stop responding. With this update, the "Cancel" button has been removed from the dialog box, resolving this issue. (BZ#579707)

* Previously, selecting the "Save History As..." option from the "Edit" menu after clearing the history could cause the Konsole terminal emulator to terminate unexpectedly with a segmentation fault. This update ensures that a correct variable is used to access the current session, and selecting the "Save History As..." menu option no longer causes Konsole to crash. (BZ#580485)

* On a system with dual screens enabled, selecting the "Cascade" window placement option in the KDE Control Center and opening a new window on the second screen could cause KWin to consider the new window off screen, and thus change the window placement back to "Smart". This update corrects the window placement algorithm to take into account the position of the screens, so that the "Cascade" window placement now works on both screens. (BZ#584822)

* Due to an error in the RPM spec file, when the lm_sensors-devel package was installed, the support for lm_sensors was automatically enabled on all architectures. However, the lm_sensors packages are only built for the x86 architectures, and an attempt to rebuild the kdebase package on the Itanium architecture failed. This update corrects the spec file to enable the lm_sensors support only on x86 architectures, so that the kdebase package can now be rebuilt successfully on all supported architectures. (BZ#638849)

All users of kdebase are advised to upgrade to this updated package, which fixes these bugs.

1.73. KDENETWORK

1.73.1. RHBA-2011:0913: kdenetwork bug fix update

An updated kdenetwork package that fixes a bug is now available for Red Hat Enterprise Linux 5.

The kdenetwork package provides a collection of networking applications for the K Desktop Environment (KDE).

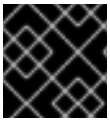
This update fixes the following bug:

* Previously, the krfb utility providing a remote desktop in KDE terminated unexpectedly when it disconnected from a remote VNC client. With this update, a patch has been provided, and krfb no longer crashes in the described scenario. (BZ#715389)

All users of kdenetwork are advised to upgrade to this updated package, which fixes this bug.

1.74. KERNEL

1.74.1. RHSA-2012:0007: Important: kernel security, bug fix, and enhancement update



IMPORTANT

This update has already been released as the security errata RHSA-2012:0007.

Updated kernel packages that fix multiple security issues, several bugs, 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 important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links after each description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security fixes:
A buffer overflow flaw was found in the way the Linux kernel's XFS file system implementation handled links with overly long path names. A local, unprivileged user could use this flaw to cause a denial of service or escalate their privileges by mounting a specially-crafted disk. (CVE-2011-4077, Important)

The fix for CVE-2011-2482 provided by RHSA-2011:1212 introduced a regression: on systems that do not have Security-Enhanced Linux (SELinux) in Enforcing mode, a socket lock race could occur between sctp_rcv() and sctp_accept(). A remote attacker could use this flaw to cause a denial of service. By default, SELinux runs in Enforcing mode on Red Hat Enterprise Linux 5. (CVE-2011-4348, Important)

The proc file system could allow a local, unprivileged user to obtain sensitive information or possibly cause integrity issues. (CVE-2011-1020, Moderate)

A missing validation flaw was found in the Linux kernel's m_stop() implementation. A local, unprivileged user could use this flaw to trigger a denial of service. (CVE-2011-3637, Moderate)

A flaw was found in the Linux kernel's Journaling Block Device (JBD). A local attacker could use this flaw to crash the system by mounting a specially-crafted ext3 or ext4 disk. (CVE-2011-4132, Moderate)

A flaw was found in the Linux kernel's encode_share_access() implementation. A local, unprivileged user could use this flaw to trigger a denial of service by creating a regular file on an NFSv4 (Network File System version 4) file system via mknod(). (CVE-2011-4324, Moderate)

A flaw was found in the Linux kernel's NFS implementation. A local, unprivileged user could use this flaw to cause a denial of service. (CVE-2011-4325, Moderate)

A missing boundary check was found in the Linux kernel's HFS file system implementation. A local attacker could use this flaw to cause a denial of service or escalate their privileges by mounting a specially-crafted disk. (CVE-2011-4330, Moderate)

Red Hat would like to thank Kees Cook for reporting CVE-2011-1020, and Clement Lecigne for reporting CVE-2011-4330.

Bug fixes:

BZ#741877

The Intel i350 Gigabit Network adapters failed to pass traffic in SR-IOV (Single Root I/O Virtualization) mode because multiple RX queues were being used, which the hardware does not support in this mode. With this update, the number of RX queues is now limited to one if SR-IOV gets enabled.

BZ#752735

Previously, link power down could not be used. The code for it was already in place but was disabled. With this update, link power down has been enabled in the code and works as expected.

BZ#755482

In some cases, a client skipped issuing a **COMMIT** call to the server when it determined that it will need to do another such call in the near future. Consequently, the NFS code failed to re-mark the inode as dirty, and the VFS file system failed to issue the call on the next pass. The inode had pages that needed to be cleaned but the inode itself was not marked as dirty. The **kdump** tuned writeback thresholds to a very low value in order to keep the page cache small. In this environment, the above bug often caused the client to become unresponsive when writing out the vmcore file. With this update, an upstream patch has been provided to address this issue and the hangs no longer occur.

BZ#759387

The IDE error handling code uses the IDE interrupt handler and the general interrupt handler. This could lead to the erroneous execution of **kexec/kdump** code that was intended to only run at boot time. As a result, the asserted IDE IRQ line would be cleared without the interrupt being handled, which in turn caused the system to become unresponsive during the shut down of the **kexec/kdump** kernel. To fix this bug, a new test for the IRQ status, which should be **IRQ_DISABLED**, has been introduced to ensure that the code introduced for the **kexec/kdump** kernel only executes at boot time.

BZ#750460

When the SMP (Symmetric Multi Processing) kernel ran the **crash_kexec()** function, the local Advanced Programmable Interrupt Controllers (APICs) could have pending interrupt requests (IRQs) in their vector tables. If there was more than one pending IRQ within the same 32-bit word in the Local APIC (LAPIC) vector table registers, the I/O APIC subsystem would enter setup with pending interrupts left in the LAPIC, causing various degrees of malfunctioning depending on the stuck interrupt vector. This update adds the **MAX_LOOPS** parameter to limit number of iterations and to provide enough time for the pending IRQs to be cleared if the loop was to lock-up for whatever reason, thus fixing this bug.

BZ#766803

Previously, the **domain_update_iommu_coherency()** function set domains, by default, as coherent when the domain was not attached to any input/output memory management units (IOMMUs). Consequently, such a domain could update context entries non-coherently via the **domain_context_mapping_one()** function. To resolve this issue, **domain_update_iommu_coherency()** has been updated to use the safer default value and domains not attached to any IOMMU are now set as non-coherent.

BZ#746343

If management firmware is present and a device is down, the firmware assumes control of the phy register. Previously, phy access was allowed from the host and it collided with firmware phy accesses, resulting in unpredictable behavior such as BMC (Baseboard Management Controller) LAN link being lost over time. With this update, the bug is fixed in the tg3 driver by only allowing phy accesses while the driver has control of the device.

BZ#744147

In certain circumstances, the `evdev_pass_event()` function with a spinlock attached was interrupted and called again, eventually resulting in a deadlock. A patch has been provided to address this issue by disabling interrupts when the spinlock is obtained. This prevents the deadlock from occurring.

BZ#750458

The unsolicited frame control infrastructure requires a table of DMA addresses for the hardware to look up the frame buffer location by an index. The hardware expects the elements of this table to be 64-bit quantities. Previously, the dma_addr_t parameter was wrongly used to reference these elements. Consequently, all unsolicited frame protocols were affected, particularly SATA-PIO and SMP, which prevented direct-attached SATA drives and expander-attached drives from being discovered. A patch has been provided to address this issue and SATA drives are now recognized correctly on 32-bit platforms.

BZ#755483

A previous patch introduced with BZ#732775 had the following unintended consequence: if no poll method was defined for files in the `/proc/` directory, processes could become unresponsive while they were reading files from this directory. This update restores the default poll behaviour for files in `/proc/` that do not have any poll method defined, thus fixing this bug.

Note that procfs files are not real files and unless they may specifically produce more data after a time (such as `/proc/kmsg`), they should not be polled for more data as some of them cannot be polled for reading. For the most part, all the data they can produce are instantly available.

BZ#754129

When directories mounted on a server are rearranged, they may then nest in a different order and clients may become unable to see or reassign the directories properly. Previously, the `__d_unalias()` and `__d_materialise_dentry()` functions did not provide loop prevention. As a consequence, NFS threads sometimes became unresponsive upon encountering a loop in the dentry tree. To fix this bug, this update adds additional loop checks and if a process tries to access a dentry that would otherwise cause the kernel to complete the loop, the **ELOOP** error code is returned and a message is logged.

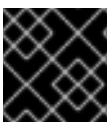
Enhancements:

BZ#758024

With this update, the latest cciss driver has been provided, which adds support for new HP Smart Array controllers.

Users should upgrade to these updated packages, which contain backported patches to fix these issues and add this enhancement. The system must be rebooted for this update to take effect.

1.74.2. RHSA-2011:1479: Important: kernel security, bug fix, and enhancement update



IMPORTANT

This update has already been released as the security errata RHSA-2011:1479.

Updated kernel packages that fix multiple security issues, several bugs, 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 important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links after each description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security fixes:
Using PCI passthrough without interrupt remapping support allowed Xen hypervisor guests to generate MSI interrupts and thus potentially inject traps. A privileged guest user could use this flaw to crash the host or possibly escalate their privileges on the host. The fix for this issue can prevent PCI passthrough working and guests starting. Refer to Red Hat Bugzilla bug 715555 for details. (CVE-2011-1898, Important)

A flaw was found in the way CIFS (Common Internet File System) shares with DFS referrals at their root were handled. An attacker on the local network who is able to deploy a malicious CIFS server could create a CIFS network share that, when mounted, would cause the client system to crash. (CVE-2011-3363, Moderate)

A NULL pointer dereference flaw was found in the way the Linux kernel's key management facility handled user-defined key types. A local, unprivileged user could use the `keyctl` utility to cause a denial of service. (CVE-2011-4110, Moderate)

A flaw in the way memory containing security-related data was handled in `tpm_read()` could allow a local, unprivileged user to read the results of a previously run TPM command. (CVE-2011-1162, Low)

A NULL pointer dereference flaw was found in the Linux kernel's HFS file system implementation. A local attacker could use this flaw to cause a denial of service by mounting a disk that contains a specially-crafted HFS file system with a corrupted MDB extent record. (CVE-2011-2203, Low)

The I/O statistics from the taskstats subsystem could be read without any restrictions. A local, unprivileged user could use this flaw to gather confidential information, such as the length of a password used in a process. (CVE-2011-2494, Low)

Red Hat would like to thank Yogesh Sharma for reporting CVE-2011-3363; Peter Huewe for reporting CVE-2011-1162; Clement Lecigne for reporting CVE-2011-2203; and Vasiliy Kulikov of Openwall for reporting CVE-2011-2494.

Bug fixes:

BZ#749459

Previously, when the `iput()` function was called while it held the `nfs_access_lru` lock could result in problems since `iput()` can sleep, and it can also attempt to allocate memory. This update removes an optimisation that is not present in the mainline kernel series. Now, `iput()` is never called while holding a spinlock in the `nfs_access_cache_shrinker()` function, thus preventing this bug.

BZ#750848

Under certain circumstances, a deadlock could occur between the khubd process of the USB stack and the modprobe of the usb-storage module. This was because the khubd process, when attempting to delete a USB device, waited for the reference count of knode_bus to be of value 0. However, modprobe, when loading the usb-storage module, scans all USB devices and increments

the reference count, preventing the khubd process from continuing. With this update, the underlying source code has been modified to address this issue, and a deadlock no longer occurs in the described scenario.

BZ#745726

A previously applied patch (introduced as a fix in CVE-2011-1898) prevented PCI pass-through inside the **`assign_device`** domctl via a security check. Because the security check was not included in the **`test_assign_device`** domctl, **`qemu-dm`** could not handle any failures in the **`test_assign_device`** domctl, ultimately causing an HVM guest to have a partly accessible PCI device, which in come cases resulted in a crash of the host machine. With this update, the security check introduced in CVE-2011-1898 has been replicated in the **`test_assign_device`** domctl, thus fixing this issue.

BZ#741273

In error recovery, most SCSI error recovery stages send a TUR (Test Unit Ready) command for every bad command when a driver error handler reports success. When several bad commands pointed to a same device, the device was probed multiple times. When the device was in a state where it did not respond to commands even after a recovery function returned success, the error handler had to wait for the commands to time out. This significantly impeded the recovery process. With this update, SCSI mid-layer error routines to send test commands have been fixed to respond once per device instead of once per bad command, thus reducing error recovery time considerably.

BZ#750451

When an INIT_ACK packet is sent with no STATE COOKIE mandatory parameter, the expected abort error cause is **`Mandatory Parameter missing`**. Previously, the **`Invalid mandatory parameter`** error cause was given instead. With this update, a bug in the **`sctp_process_missing_param()`** function has been fixed and now, correct error cause value for missing parameters is set in the described scenario.

BZ#750457

When a COOKIE_ACK message with a packet length smaller then the chunk length defined was received, SCTP (Stream Control Transmission Protocol) sent an ABORT message with incorrectly encoded PROTOCOL VIOLATION error cause. With this update, the underlying code has been fixed and the ABORT message is now encoded properly in the described scenario.

BZ#750842

Due to a regression, the byte count on the wrong buffer was adjusted to account for endian differences. This resulted in the wrong buffer length being passed to the callers on big endian machines, which in turn resulted in data returned from the server being incorrectly rejected with "Invalid transact2 SMB: " error messages. This bug was first reported on the 64-bit PowerPC architecture. With this update, the correct buffer length is now passed in the described scenario.

BZ#750841

Previously, if a connect change occurs on a USB device, it is reported the same way as a disconnect. As a consequence, the "hub 1-1.6:1.0: Cannot enable port X. Maybe the USB cable is bad?" were issued by the dmesg utility when a low speed USB device was connected to port X. With this update, the port reset code in the hub driver has been changed, code of the **`usb_reset_device()`** function has been fixed to prevent the routine from futilely retrying the reset after a disconnect has occurred, and no error messages are now returned in the described scenario.

BZ#744700

The operational state of a network device, represented by the value in **/sys/class/net/eth<*X*>/operstate**, was not initialized by default and reported **unknown** when the network device was up and was using the **tg3** driver. This update fixes the **tg3** driver to properly set the ***operstate*** value.

BZ#750912

The **be2net** driver does not use lock-less Tx paths and its **xmit()** function is protected by the **netif_tx_lock** spinlock; as are the **set_multicast_list()** and **set_rx_mode()** functions. This configuration setup involves sending a message to the card firmware and getting a reply back, which involves delay up to several miliseconds long. As a consequence, the requeue counter increased by high numbers. With this update, the **NETIF_F_LLTX** feature has been enabled and locking of own Tx paths has been implemented. Now, only small portions of multicast configuration needs to be locked in the described scenario.

BZ#743611

Prior to this update, the **ndisc_send_skb()** function was using an incorrect macro to increment the ICMP6 statistics. As a result, an out-of-bound element in an array which resides in the size-128 slab pool was incremented, causing data corruption. If the array was near the end of the slab page, user data corruption could occur. This update fixes the above-mentioned function to use the correct macro for incrementing the ICMP6 statistics, and data corruption no longer occurs.

BZ#742282

A previously introduced patch reduced the size of the DMA zone under the Xen hypervisor. Consequently, drivers trying to allocate contiguous memory with the **dma_alloc_coherent()** API often had their requests fail. This resulted in BIOS update failures on some systems with large flash memory. With this update, the zone restriction in **dma_alloc_coherent()** is relaxed, thus fixing this issue.

BZ#747872

When the hangcheck timer expires and tries to reboot the machine, it stops all other CPUs in the configuration. However, the CPU that stops the other CPUs is still enabled for interrupts. Consequently, I/O or external interrupts might arrive at the local CPU and the corresponding interrupt handler might try to acquire a lock. Previously, if a remote CPU was holding the lock while the local CPU stopped it, the result was a deadlock. The system became unresponsive instead of performing a reboot. With this update, interrupts are disabled before stopping remote CPUs and the hangs no longer occur in the described scenario.

BZ#747876

On IBM System z, if a Linux instance with large amounts of anonymous memory runs into a memory shortage the first time, all pages on the active or inactive lists are considered referenced. This causes the memory management on IBM System z to do a full check over all page cache pages and start writeback for all of them. As a consequence, the system became temporarily unresponsive when the described situation occurred. With this update, only pages with active mappers are checked and the page scan now does not cause the hangs.

BZ#750477

Previously, kernel was allowed to reduce the number of unnecessary commit calls by skipping the commit when there was a large number of outstanding pages being written. However, that test did not properly handle the edge case when the number of commits (ncommit) was zero. Consequently, inodes sometimes remained on the **sb->s_dirty** list and could not be freed by the inode cache

shrinker. As a result, the **nfs_inode_cache** structure grew very large over time. With this update, the call to the **nfs_write_inode()** function is immediately returned when **commit == 0**, thus fixing this bug.

BZ#750508

A previous kernel patch removed a call in the **nfs_file_release()** function to the **filemap_fdatawrite()** function. Consequently, data written to a NFS file, which had been mapped into memory via the **mmap()** function and not yet flushed to the backing device, were lost as soon as the file was closed. This update adds the **filemap_fdatawrite()** call back to the **nfs_file_flush()** function, which fixes this regression.

BZ#746600

The Xen network back-end driver was supposed to turn on all of its possible features until it negotiated with the front-end. However, after the negotiation, it did not disable the features declined by the front-end. This caused Windows guest using the **xenpv-win** network driver to not be able to transmit data to the host over TCP. This update properly disables the features which are not supported by the front-end.

Enhancement

BZ#743806

This update improves the performance of delete/unlink operations in a **GFS2** file system containing large files by adding a layer of metadata read-ahead for indirect blocks.

Users should upgrade to these updated packages, which contain backported patches to correct these issues and add this enhancement. The system must be rebooted for this update to take effect.

1.74.3. RHSA-2011:1212: Important: kernel security and bug fix update

IMPORTANT

This update has already been released as the security errata RHSA-2011:1212.

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.

Security fixes:
A NULL pointer dereference flaw was found in the Linux kernel's 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-2011-2482, Important)

A flaw in the Linux kernel's client-side NFS Lock Manager (NLM) implementation could allow a local, unprivileged user to cause a denial of service. (CVE-2011-2491, Important)

Buffer overflow flaws in the Linux kernel's netlink-based wireless configuration interface

implementation could allow a local user, who has the CAP_NET_ADMIN capability, to cause a denial of service or escalate their privileges on systems that have an active wireless interface. (CVE-2011-2517, Important)

A flaw was found in the way the Linux kernel's Xen hypervisor implementation emulated the SAHF instruction. When using a fully-virtualized guest on a host that does not use hardware assisted paging (HAP), such as those running CPUs that do not have support for (or those that have it disabled) Intel Extended Page Tables (EPT) or AMD Virtualization (AMD-V) Rapid Virtualization Indexing (RVI), a privileged guest user could trigger this flaw to cause the hypervisor to crash. (CVE-2011-2519, Moderate)

An off-by-one flaw was found in the **`__addr_ok()`** macro in the Linux kernel's Xen hypervisor implementation when running on 64-bit systems. A privileged guest user could trigger this flaw to cause the hypervisor to crash. (CVE-2011-2901, Moderate)

`/proc/<PID>/io` is world-readable by default. Previously, these files could be read without any further restrictions. A local, unprivileged user could read these files, belonging to other, possibly privileged processes to gather confidential information, such as the length of a password used in a process. (CVE-2011-2495, Low)

Red Hat would like to thank Vasily Averin for reporting CVE-2011-2491, and Vasiliy Kulikov of Openwall for reporting CVE-2011-2495.

Bug fixes:

BZ#719746

Prior to this update, a race condition in TIPC's (Transparent Inter-process Communication) **`recv_msg`** function caused kernel panic. This update modifies TIPC's socket locking logic, and kernel panic no longer occurs.

BZ#722855

The RHSA-2009:1243 update introduced a regression in the way file locking on NFS (Network File System) was handled. This caused applications to hang if they made a lock request on a file on an NFS version 2 or 3 file system that was mounted with the **`sec=krb5`** option. With this update, the original behavior of using mixed RPC authentication flavors for NFS and locking requests has been restored.

BZ#726625

An incorrect call to the **`nfs4_drop_state_owner`** function caused the NFSv4 state reclaimer thread to be stuck in an infinite loop while holding the Big Kernel Lock (BKL). With this update, the aforementioned call has been removed, thus, fixing this issue.

BZ#728163

Certain systems do not correctly set the ACPI FADT APIC mode bit. They set the bit to "cluster" mode instead of "physical" mode which caused these systems to boot without the TSC. With this update, the ACPI FADT check has been removed due to its unreliability, thus, fixing this issue.

BZ#712885

A bug was found in the way the **`x86_emulate()`** function handled the ***`IMUL`*** instruction in the Xen hypervisor. On systems without support for hardware assisted paging (HAP), such as those running CPUs that do not have support for (or those that have it disabled) Intel Extended Page Tables (EPT) or AMD Virtualization (AMD-V) Rapid Virtualization Indexing (RVI), this bug could cause fully-

virtualized guests to crash or lead to silent memory corruption. In reported cases, this issue occurred when booting fully-virtualized Red Hat Enterprise Linux 6.1 guests with memory cgroups enabled on a Red Hat Enterprise Linux 5.7 host.

BZ#727592

The fix provided in CVE-2010-3432 information in **`sctp_packet_config()`**, which is called before appending data chunks to a packet, was no longer reset, ultimately causing performance issues. With this update, packet information is reset after a packet transmit, thus, fixing the aforementioned performance issues.

BZ#721300

Prior to this update, an attempt to use the **`vfree()`** function on a **`vmalloc()`**'ed area could result in a memory leak. With this update, the underlying source code has been modified to address this issue, and a memory leak no longer occurs.

BZ#727590

A problem with the XFS dio error handling was discovered. If a misaligned write I/O operation was issued, XFS would return ***`-EINVAL`*** without unlocking the inode's mutex. This caused any further operations on the inode to become unresponsive. This update adds a missing **`mutex_unlock`** operation to the dio error path, solving this issue.

BZ#726619

Older versions of be2net cards firmware may not recognize certain commands and return illegal/unsupported errors, causing confusing error messages to appear in the logs. With this update, the driver handles these errors gracefully and does not log them.

BZ#723552

This patch fixes the inability of the be2net driver to work in a kdump environment. It clears an interrupt bit (in the card) that may be set while the driver is probed by the kdump kernel after a crash.

BZ#726628

When a block device object was allocated, the **`bd_super`** field was not being explicitly initialized to **`NULL`**. Previous users of the block device object may have set the **`bd_super`** field to **`NULL`** when the object is released by calling the **`kill_block_super()`** function. Some third party file systems do not always use this function and as a result the **`bd_super`** field could have become uninitialized when the object was allocated again. This could cause a kernel panic in the **`blkdev_releasepage()`** function when the uninitialised **`bd_super`** field was dereferenced. With this update, the **`bd_super`** field is properly initialized in the **`bdget`** function, and kernel panic no longer occurs.

BZ#727835

Under some circumstances, error reports within the XFS file system could dereference a NULL pointer cause kernel panic. This update fixes the NULL pointer dereference, and kernel panic no longer occurs

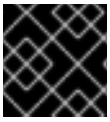
BZ#719930

This update makes the size of the three DLM hash tables consistent: 1024 entries with a Red Hat Enterprise Linux 5-specific change to allocate the tables using **`vmalloc`** allowing a higher maximum size that can be allocated for these tables. This results in improved DLM/GFS

performance when there are many locks being held (that is, many GFS files being used).

Users should upgrade to these updated packages, which contain backported patches to correct these issues, and fix these bugs. The system must be rebooted for this update to take effect.

1.74.4. RHSA-2011:1065: Important Red Hat Enterprise Linux 5.7 kernel security and bug fix update



IMPORTANT

This update has already been released as the security errata RHSA-2011:1065.

Updated kernel packages that fix multiple 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 seventh 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 after each description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security fixes:
A flaw was found in the way the Xen hypervisor implementation handled instruction emulation during virtual machine exits. A malicious user-space process running in an SMP guest could trick the emulator into reading a different instruction than the one that caused the virtual machine to exit. An unprivileged guest user could trigger this flaw to crash the host. This only affects systems with both an AMD x86 processor and the AMD Virtualization (AMD-V) extensions enabled. (CVE-2011-1780, Important)

A flaw allowed the `tc_fill_qdisc()` function in the Linux kernel's packet scheduler API implementation to be called on built-in qdisc structures. A local, unprivileged user could use this flaw to trigger a NULL pointer dereference, resulting in a denial of service. (CVE-2011-2525, Moderate)

A flaw was found in the way space was allocated in the Linux kernel's Global File System 2 (GFS2) implementation. If the file system was almost full, and a local, unprivileged user made an `fallocate()` request, it could result in a denial of service. Note: Setting quotas to prevent users from using all available disk space would prevent exploitation of this flaw. (CVE-2011-2689, Moderate)

Bug Fixes:

BZ#704735

The `be2iscsi` driver passed a local variable in the `request_irq` function which lead to corruption in `/proc/interrupts`. All data in `/proc/interrupts` was correct except the device names. This update fixes the incorrect devices names in `/proc/interrupts`.

BZ#660871

Calling the `mptctl_fasync()` function to enable async notification caused the `fasync_struct` data structure, which was allocated, to never be freed. `fasync_struct` remained on the event list of the `mptctl` module even after a file was closed and released. After the file was closed, `fasync_struct` had an invalid file pointer which was dereferenced when the `mptctl` module called the `kill_fasync()` function to report any events. The use of the invalid file pointer could

result in a deadlock on the system because the **send_sigio()** function tried to acquire the ***rwlock*** in the ***f_owner*** field of the previously closed file. With this update, a release *callback* function has been added for the file operations in the **mptctl** module. **fasync_struct** is now properly freed when a file is closed, no longer causing a deadlock.

BZ#665427

If an error occurred during I/O, the SCSI driver reset the **megaraid_sas** controller to restore it to normal state. However, on Red Hat Enterprise Linux 5, the waiting time to allow a full reset completion for the **megaraid_sas** controller was too short. The driver incorrectly recognized the controller as stalled, and, as a result, the system stalled as well. With this update, more time is given to the controller to properly restart, thus, the controller operates as expected after being reset.

BZ#695493

On a Red Hat Enterprise Linux 5.7 system, it is advisable to update the firmware of the HP ProLiant Generation 6 (G6) controller's firmware to version 5.02 or later. Once the firmware is successfully updates, reboot the system and **kdump** will work as expected.

HP G6 controllers include: P410i, P411, P212, P712, and P812.

In addition, **kdump** may fail when using the HP Smart Array 5i Controller on a Red Hat Enterprise Linux 5.7 system.

BZ#696153

Under certain circumstances, a command could have been left unprocessed when using either the **cciss** or **hpsa** driver because the HP Smart Array controller considered those commands to be completed when, in fact, they were still waiting in the completion queue. This could have caused the file system to become read-only or panic, and the whole system to become unstable. This update adds an extra read operation to both the **cciss** and **hpsa** drivers, with the result that commands in the completion queue are properly processed.

BZ#646513

A call to the **HP_GETHOSTINFO** ioctl (I/O Control) in the **mptctl** module could result in the MPT (Message Passing Technology) fusion driver being reset due to erroneous detection of completed ioctl commands. With this update, the message context sent to the **mptctl** module is stored (previously, it was zeroed). When an ioctl command completes, the saved message context is used to recognize the completion of the message, thus resolving the faulty detection.

BZ#664592

Using the **cciss** driver, when a TUR (Test Unit Ready) was executed, the ***rq->bio*** pointer in the **blk_rq_bytes** function was of value *null*, which resulted in a null pointer dereference, and, consequently, kernel panic occurred. With this update, the ***rq->bio*** pointer is used only when the **blk_fs_request(rq)** condition is true; thus, kernel panic no longer occurs.

BZ#706244

Using the **megaraid_sas** driver, if a user configured 2 logical disks on a RAID volume whose disks are larger than 2 TB, with the start of the second logical disk after the 2 TB mark, and FastPath was enabled, FastPath read operations to the second logical disk were read from the incorrect location on disk. However, write operations were not affected and were always directed to the correct disk location. With this update, the driver detects if **LBA > 0xffffffff & cdb_len < 16**, then converts the **cdb** from the OS to a 16 byte CDB, before firing it as a FastPath I/O, fixing this issue.

BZ#656032

Due to incorrect ordering of glocks, a deadlock could occur in the code which reclaims unlinked inodes when multiple nodes were trying to deallocate the same unlinked inode. This update resolves the lock ordering issue, and unlinked inodes are now properly deallocated under all circumstances.

BZ#669527

The **bnx2i** driver could cause a system crash on IBM POWER7 systems. The driver's page tables were not set up properly on Big Endian machines, causing extended error handling (EEH) errors on PowerPC machines. With this update, the page tables are properly set up, and a system crash no longer occurs in the aforementioned case.

BZ#700203, BZ#673616

VDSO (Virtual Dynamically-linked Shared Object) kernel variables must be exported in **vextern.h**, otherwise they end up as undefined pointers. When calling the VDSO **gettimeofday()** function in Red Hat Enterprise Linux 5, a missing declaration lead to a segmentation fault. With this update, the **sysctl_vsyscall** system call is properly exported, and segmentation faults no longer occur.

BZ#660661

Due to an off-by-one error, **gfs2_grow** failed to take the very last ***rgrp*** parameter into account when adding up the new free space. With this update, the GFS2 kernel properly counts all the new resource groups and fixes the **statfs** file correctly.

BZ#683155

GFS2 (Global File System 2) keeps track of the list of resource groups to allow better performance when allocating blocks. Previously, when the user created a large file in GFS2, GFS2 could have run out of allocation space because it was confined to the recently-used resource groups. With this update, GFS2 uses the MRU (Most Recently Used) list instead of the list of the recently-used resource groups. The MRU list allows GFS2 to use all available resource groups and if a large span of blocks is in use, GFS2 uses allocation blocks of another resource group.

BZ#690555

Multiple GFS2 nodes attempted to unlink, rename, or manipulate files at the same time, causing various forms of file system corruption, panics, and withdraws. This update adds multiple checks for dinode's ***i_nlink*** value to assure inode operations such as link, unlink, or rename no longer cause the aforementioned problems.

BZ#694669

Prior to this update, a race in the GFS2 glock state machine could cause nodes to become unresponsive. Specifically, all nodes but one would hang, waiting for a particular glock. All the waiting nodes had the W (Waiting) bit set. The remaining node had the glock in the Exclusive Mode (EX) with no holder records. The race was caused by the Pending Demote bit, which could be set and then immediately reset by another process. With this update, the Pending Demote bit is properly handled, and GFS2 nodes no longer hang.

BZ#691460

Certain IBM storage arrays, such as the IBM 1745 and 1746, could have stopped responding or failed to load the device list of the **scsi_dh_rdac** kernel module. This occurred because the **scsi_dh_rdac** device list did not contain these storage arrays. With this update, the arrays have been added to the list, and they are now detected and operate as expected.

BZ#665197

Prior to this update, the following message was displayed when booting a Red Hat Enterprise Linux 5 system on a virtual guest:

```
WARNING calibrate_APIC_clock: the APIC timer calibration may be wrong.
```

This was due to the ***MAX_DIFFERENCE*** parameter value (in the APIC calibration loop) of 1000 cycles being too aggressive for virtual guests. APIC (Advanced Programmable Interrupt Controllers) and TSC (Time Stamp Counter) reads normally take longer than 1000 cycles when performed from inside a virtual guest, due to processors being scheduled away from and then back onto the guest. With this update, the ***MAX_DIFFERENCE*** parameter value has been increased to 10,000 for virtual guests.

BZ#675727

Prior to this update, a segmentation fault occurred when an application called VDSO's **`gettimeofday()`** function due to erroneous exporting of the ***`wall_to_monotonic`*** construct. With this update, the ***`wall_to_monotonic`*** construct is correctly exported, and a crash no longer occurs.

BZ#675793

A cpu mask that is being waited on after an IPI call was not the same cpu mask that was being passed into the IPI call function. This could result in not up-to-date values being stored in the cache. The loop in the **`flush_tlb_others()`** function waited for the cpu mask to be cleared, however, that cpu mask could have been incorrect. As a result, the system could become unresponsive. With this update, the cpu mask being waited on is the same cpu mask used in the IPI call function, and the system no longer hangs.

BZ#659594

A bug was discovered in the bonding driver that occurred when using netpoll and changing, adding or removing slaves from a bond. The misuse of a per-cpu flag in the bonding driver during these operations at the wrong time could lead to the detection of an invalid state in the bonding driver, triggering kernel panic. With this update, the use of the aforementioned per-cpu flag has been corrected and a kernel panic no longer occurs.

BZ#692921

The **kdump** kernel could fail when handling an IPI (Inter-processor interrupt) that was in-flight as the initial kernel crashed. This was due to an IPI-related data structure within **kdump**'s kernel not being properly initialized, resulting in a dereference of an invalid pointer. This update addresses this issue, and the **kdump** kernel no longer fails upon encountering an in-flight IPI.

BZ#669961

For a device that used a Target Portal Group (TPG) ID which occupied the full 2 bytes in the RTPG (Report Target Port Groups) response (with either byte exceeding the maximum value that may be stored in a signed char), the kernel's calculated TPG ID would never match the group_id that it should. As a result, this signed char overflow also caused the ALUA handler to incorrectly identify the AAS (Asymmetric Access State) of the specified device as well as incorrectly interpret the supported AAS of the target. With this update, the aforementioned issue has been addressed and no longer occurs.

BZ#673058

A race could occur when an internal **multipath** structure (**`pgpath`**) was freed before it was used to

signal the path group initialization was complete (via **pg_init_done**). This update includes a number of fixes that address this issue. **multipath** is now increasingly robust when **multipathd** restarts are combined with I/O operations to **multipath** devices and storage failures.

BZ#680561

The event device (**evdev**) failed to lock data structures when adding or removing input devices. As a result, kernel panic occurred in the **evdev_release** function during a system restart. With this update, locking of data structures works as expected, and kernel panic no longer occurs.

BZ#670373

Prior to this update, kernel panic occurred in the **kfree()** due to a race condition in the **acpi_bus_receive_event()** function. The **acpi_bus_receive_event()** function left the ***acpi_bus_event_list*** list attribute unlocked between checking it whether it was empty and calling the **kfree()** function on it. With this update, a check was added after the lock has been lifted in order to prevent the race and the calling of the **kfree()** function on an empty list.

BZ#677703

Running a reboot test on an iSCSI root host resulted in kernel panic. When the **iscsi_tcp** module is destroying a connection it grabs the ***sk_callback_lock*** and clears the ***sk_user_data/conn*** pointer to signal that the callback functions should not execute the operation. However, some functions were not grabbing the lock, causing a NULL pointer kernel panic when **iscsi_sw_tcp_conn_restore_callbacks** was called and, consequently, one of the callbacks was called. With this update, the underlying source code has been modified to address this issue, and kernel panic no longer occurs.

BZ#664931

Prior to this update, a multi-threaded application, which invoked **popen(3)** internally, could cause a thread stall by FILE lock corruption. The application program waited for a FILE lock in **glibc**, but the lock seemed to be corrupted, which was caused by a race condition in the COW (Copy On Write) logic. With this update, the race condition was corrected and FILE lock corruption no longer occurs.

BZ#667673

The ext4 file system could end up corrupted after a power failure occurred even when file system barriers and local write cache was enabled. This was due to faulty barrier flag setting in **WRITE_SYNC** requests. With this update, this issue has been fixed, and ext4 file system corruption no longer occurs.

BZ#627496

When selecting a new window, the **tcp_select_window()** function tried not to shrink the offered window by using the maximum of the remaining offered window size and the newly calculated window size. The newly calculated window size was always a multiple of the window scaling factor, however, the remaining window size was not since it depended on ***rcv_wup/rcv_nxt***. As a result, a window was shrunk when it was scaled down. With this update, aligning the remaining window to the window scaling factor assures a window is no longer shrunk.

BZ#695369

Configuring a network bridge with no STP (Spanning Tree Protocol) and a 0 forwarding delay could result in the flooding of all packets on the link for 20 seconds due to various issues in the source code. With this update, the underlying source code has been modified to address this issue, and a traffic flood on the network bridge no longer occurs.

BZ#646816

Prior to this update, the **/proc/diskstats** file showed erroneous values. This occurred when the kernel merged two I/O operations for adjacent sectors which were located on different disk partitions. Two merge requests were submitted for the adjacent sectors, the first request for the second partition and the second request for the first partition, which was then merged to the first request. The first submission of the merge request incremented the *in_flight* value for the second partition. However, at the completion of the merge request, the *in_flight* value of a different partition (the first one) was decremented. This resulted in the erroneous values displayed in the **/proc/diskstats** file. With this update, the merging of two I/O operations which are located on different disk partitions has been fixed and works as expected.

BZ#643441

If an application opened a file with the **O_DIRECT** flag on an NFS client and performed write operations on it of size equal to ***wsize*** (size of the blocks of data passed between the client and the server), the NFS client sent two RPCs (Remote Procedure Calls) when only one RPC needed to be send. Write operations of size smaller than ***wsize*** worked as expected. With this update, write operations of size equal to ***wsize*** now work as expected and no longer cause the NFS client to send out unnecessary RPCs.

BZ#653286

Under certain circumstances, a crash in the kernel could occur due to a race condition in the **lockd_down** function, which did not wait for the **lockd** process to come down. With this update, the **lockd_down** function has been fixed, and the kernel no longer crashes.

BZ#671595

Prior to this update, the **be2net** driver failed to work with bonding, causing *flapping* errors (the interface switches between states up and down) in the active interface. This was due to the fact that the ***netdev->trans_start*** pointer in the **be_xmit** function was not updated. With this update, the aforementioned pointer has been properly updated and *flapping* errors no longer occur.

BZ#664705, **BZ#664707**

For certain NICs, the ***operstate*** state (stored in, for example, the **/sys/class/net/eth0/operstate** file) was showing the unknown state even though the NIC was working properly. This was due to the fact that at the end of a probe operation, the **netif_carrier_off** was not being called. With this update, the **netif_carrier_off** is properly called after a probe operation, and the ***operstate*** state now correctly displays the operational state of an NIC.

BZ#506630

RHEL5.7 has introduced the new multicast snooping feature for virt bridge. The feature is disabled by default in order to not break any existing configurations. To enable the feature, please set the tunnable parameter below to **1**:

```
/sys/class/net/breth0/bridge/multicast_snooping
```

Please also note that with multicast snooping enabled, it may caused a regression with some switches where it causes a break in the multicast forwarding for some peers.

BZ#661110

Outgoing packets were not fragmented after receiving the **icmpv6 pkt-too-big** message when

using the IPSecv6 tunnel mode. This was due to the lack of IPv6 fragmentation support over an IPsec tunnel. With this update, IPv6 fragmentation is fully supported and works as expected when using the IPSecv6 tunnel mode.

BZ#667234

The fix introduced with BZ#560013 added a check for detection of the **`northbridge`** device into the **`amd_fixup_dcm()`** function to make Red Hat Enterprise Linux 5 guests boot on a 5.4.z Xen hypervisor. However, the added check caused a kernel panic due to missing multi-node CPU topology detection on AMD CPU family 0x15 systems. To preserve backwards compatibility, the check has not been removed but is triggered only on AMD Family 15h systems (code-named "Magny-Cours"). AMD family 0x15 systems do not require the aforementioned check because they are not supported as 5.4 Xen Hypervisor hosts. For Xen Hypervisor 5.5, this issue has been fixed, which makes the check obsolete.

BZ#675258

Booting a Red Hat Enterprise Linux 5.4 or later kernel failed (the system became unresponsive) due to the zeroing out of extra bytes of memory of the reset vector. The reset vector is comprised of two 16-bit registers (high and low). Instead of zeroing out 32-bits, the kernel was zeroing out 64-bits. On some machines this overwritten memory was used during the boot process, resulting in a hang. With this update, the long data type has been changed to the unsigned 32-bit data type; thus, resolving the issue. The Red Hat Enterprise Linux 5.4 and later kernel now boot as expected on the machines affected by this bug.

BZ#678074

Setting the capture levels on the Line-In capture channel when using an ARX USB I/O sound card for recording and playback did not work properly. The set values were not persistent. With this update, the capture values are now cached in the **`usb-audio`** driver leaving the set capture levels unchanged.

BZ#688926

This update fixes a bug in the way isochronous input data was returned to user space for **usbfs** (USB File System) transfers, resolving various audio issues.

BZ#645431

The Red Hat Enterprise Linux kernel can now be tainted with a *tech preview* status. If a kernel module causes the tainted status, then running the command **`cat /proc/modules`** will display a **`(T)`** next to any module that is tainting the kernel.

For more information about Technology Previews, refer to:

https://access.redhat.com/support/offerings/techpreview/

Important: Running a kernel with the tainted flag set may limit the amount of support that Red Hat can provide for the system.

BZ#525898

Previously, paravirtualized Xen guests allocated all low memory (all memory for 64-bit) to **`ZONE_DMA`**, rather than using **`ZONE_DMA32`** and **`ZONE_NORMAL`**. The guest kernels now use all three zones the same way natively running kernels do.

BZ#651512

While bringing down an interface, the **`e1000`** driver failed to properly handle IRQs (Interrupt

Requests), resulting in the reception of the following messages:

```
irq NN: nobody cared...
```

With this update, the driver's down flag is set later in the process of bringing down an interface, specifically, after all timers have exited, preventing the IRQ handler from being called and exiting early without handling the IRQ.

BZ#651837

By default, **libsas** defines a wideport based on the attached SAS address, rather than the specification compliant "strict" definition of also considering the local SAS address. In Red Hat Enterprise Linux 5.7, only the default "loose" definition is available. The implication is that if an OEM configures an SCU controller to advertise different SAS addresses per PHY, but hooks up a wide target or an expander to those PHYs, **libsas** will only create one port. The expectation, in the "strict" case, is that this would result in a single controller **multipath** configuration.

It is not possible to use a single controller **multipath** without the `strict_wide_port` functionality. Multi-controller **multipath** should behave as a expected.

A x8 **multipath** configuration through a single expander can still be obtained under the following conditions:

1. Start with an SCU SKU that exposes (2) x4 controllers (total of 8 PHYs)
2. Assign ***sas_address1*** to all the PHYs on `controller1`
3. Assign ***sas_address2*** to all the PHYs on `controller2`
4. Hook up the expander across all 8 PHYs
5. Configure **multipath** across the two controller instances

It is critical for `controller1` to have a distinct address from `controller2`, otherwise the expander will be unable to correctly route connection requests to the proper initiator.

BZ#673242

Previously, on VMware, the time ran too fast on virtual machines with more than 4GHz TSC (Time Step Counter) processor frequency if they were using PIT/TSC based timekeeping. This was due to a calculation bug in the `get_hypervisor_cycles_per_sec` function. This update fixes the calculation, and timekeeping works correctly for such virtual machines.

BZ#661478

A formerly introduced patch that provided extended PCI config space access on AMD systems caused the `lpfc` driver to fail when it tried to initialize hardware. On **kernel-xen**, Hypervisor trapped the aforementioned accesses and truncated them, causing the `lpfc` driver to fail to initialize hardware. Note that this issue was only observed when using the `lpfc` driver with the following parameters: ***Vendor_ID=0x10df***, ***Device_ID=0xf0e5***. With this update, the part of the patch related to **kernel-xen** that was causing the failures was removed and the `lpfc` driver now works as expected.

BZ#698879

Hot removing a PCIe device and, consequently, hot plugging it again caused kernel panic. This was due to a PCI resource for the SR-IOV Virtual Function (vf) not being released after the hot

removing, causing the memory area in the **pci_dev** struct to be used by another process. With this update, when a PCIe device is removed from a system, all resources are properly released; kernel panic no longer occurs.

BZ#672368, BZ#695490

In a four node cluster environment, a deadlock could occur on machines in the cluster when the nodes accessed a GFS2 file system. This resulted in memory fragmentation which caused the number of network packet fragments in requests to exceed the network hardware limit. The network hardware firmware dropped the network packets exceeding this limit. With this update, the network packet fragmentation was reduced to the limit of the network hardware, no longer causing problems during memory fragmentation.

BZ#674298

Prior to this update, if a CT/ELS pass-through command timed out, the QLogic 8Gb Fibre Channel adapter created a firmware dump. With this update, firmware dumps are no longer created when CT/ELS pass-through requests time out as a firmware dump is not necessary in this case.

BZ#695357

Setting a DASD (Direct Access Storage Device) device offline while another process is trying to open that device caused a race in the **dasd_open** function. The **dasd_open** function tried to read a pointer from the private_data field after the structure has already been freed, resulting in a dereference of an invalid pointer. With this update, the aforementioned pointer is now stored in a different structure; thus, preventing the race condition.

BZ#666080

Deleting a file on a GFS2 file system caused the inode, which the deleted file previously occupied, to not be freed. Specifically, this only occurred when a file was deleted on a particular node while other nodes in the cluster were caching that same inode. The mechanism for ensuring that inodes are correctly deallocated when the final close occurs was dependent on a previously corrected bug (BZ#504188). In order to ensure that iopen glocks are not cached beyond the lifetime of the inode, and thus prevent deallocation by another inode in the cluster, this update marks the iopen glock as not to be cached during the inode disposal process.

BZ#610093

In some cases the NFS server fails to notify NFSv4 clients about renames and unlinks done by non-NFS users of the server. An application on a client may then be able to open the file at its old location (read old cached data from it and perform read locks on it), long after the file no longer exists at that location on the server. To work around this issue, use NFSv3 instead of NFSv4. Alternatively, turn off support for leases by writing the value **0** to the **/proc/sys/fs/leases-enable** file (ideally on boot, before the NFS server is started). This change prevents NFSv4 delegations from being given out, restoring correctness at the expense of some performance.

BZ#662102

Booting Red Hat Enterprise Linux 5 with the ***crashkernel=X*** parameter enabled for the **kdump** kernel does not always succeed. This is because the kernel may not be able to find a suitable memory range for the **crashkernel** due to the fragmentation of the physical memory. Similarly, if a user specifies the starting address of the reserved memory, the specified memory range may be occupied by other parts of the kernel (in this case, the **initrd**, i.e. initial ramdisk). This update adds two debugging kernel parameters (**bootmem_debug** and **ignore_loglevel**) which allow to diagnose what causes the **crashkernel** to not be assigned enough memory.

BZ#698873

In Red Hat Enterprise Linux 5.7 netconsole was enabled to work with software network bridges. This disables previous workaround used by RHEV Manager Agent (VDSM) to use ethernet network interface directly.

Customers wishing to continue using netconsole logging on the RHEL 5.7 nodes registered with RHEV Manager, should modify the **/etc/sysconfig/netconsole** file and change the line where the ***DEV*** variable is set to:

```
DEV=rhevm
```

and restart the **netconsole** service with:

```
# service netconsole restart
```

BZ#669909

Prior to this update, a rhev-agent could not be started due to missing a **/dev/virtio-ports/** directory. This was due to the fact that the **udev** utility does not parse the **KOBJ_CHANGE** event. With this update, the **KOBJ_ADD** event is invoked instead so that symlinks in **/dev/virtio-ports** are created when a port name is obtained.

BZ#673459

Using a virtio serial port from an application, filling it until the write command returns **-EAGAIN** and then executing a select command for the write command caused the select command to not return any values, when using the virtio serial port in a non-blocking mode. When used in a blocking mode, the write command waited until the host indicated it used up the buffers. This was due to the fact that the poll operation waited for the **port->waitqueue** pointer, however, nothing woke the **waitqueue** when there was room again in the queue. With this update, the queue is woken via host notifications so that buffers consumed by the host can be reclaimed, the queue freed, and the application write operations may proceed again.

BZ#653236

Prior to this update, a FW/SW semaphore collision could lead to an link establishment failure on an SFP+ (Small Form-factor Pluggable) transceiver module. With this update, the underlying source code has been modified to address this issue, and SFP+ modules work as expected.

BZ#680531

Enabling the Header Splitting mode on all Intel 82599 10 Gigabit Ethernet hardware could lead to unpredictable behavior. With this update, the Header Splitting mode is never enabled on the aforementioned hardware. Additionally, this update fixes VM pool allocation issues based on MAC address filtering, and limits the scope of VF access to promiscuous mode.

BZ#657166

Using an XFS file system, when an I/O error occurred during an intermediate commit on a rolling translation, the **xfs_trans_commit()** function freed the structure of the transaction and the related ticket. However, the duplicate transaction, which is used when the transaction continues, still contained a pointer to the freed ticket. Therefore, when the second transaction was canceled, the ticked was freed for the second time, causing kernel panic. This update adds reference counting to the ticket to avoid multiple freeing of a ticket when a commit error occurs.

BZ#616125

A spurious **BUG_ON()** call caused the ***module_refcount*** variable to not be always accurate outside of the atomic state within the **stop_machine** function, observed mainly under heavy network load. This update removed the **BUG_ON()** call, fixing this issue.

BZ#695197

A previously introduced patch added support for displaying the temperature of application-specific integrated circuits (ASIC). However, a missing increment of the ***work_counter*** variable in the **be_worker** function caused the **be_cmd_get_die_temperature** function to be called every 1 second (instead of the 32 seconds it should be), and the **be_cmd_get_die_temperature** function to be called even when it was not supported. This update fixes this issue.

BZ#695168

Prior to this update, the ***stat.st_blksize*** parameter was always set to **PAGE_CACHE_SIZE**, causing performance issues. With this update, the underlying source code has been modified to address this issue, and Red Hat Enterprise Linux 5 systems no longer suffer from performance issues caused by the aforementioned parameter.

BZ#710584

Broken *scatterlist* handling during command construction caused SMP commands to fail, resulting in the SCU driver not detecting drives behind expanders. This update fixes the SCU driver to detect drives placed behind expanders.

BZ#658012

Kernel panic occurred when a non-maskable interrupt was issued during a forced shutdown of the XFS file system. This was due to a spinlock occurring in various functions. With this update, the spinlocks have been removed, and kernel panic no longer occurs. Additionally, the **CONFIG_XFS_DEBUG** option is disabled by default on kernel-debug.

BZ#663123

Prior to this update, the **/proc/partitions** file was not being updated after LUNs were created using the **hpacucli** utility (which adds, deletes, identifies, and repairs logical and physical disks). This issue has been fixed via the update of the CCISS driver to version 3.6.26-5, as noted in BZ#635143.

BZ#704963

When the **ibmvscsi** driver reset its CRQ and attempted to re-register the CRQ, it received an H_CLOSED response, indicating that the Virtual I/O Server is not yet ready to receive commands. As a result, the **ibmvscsi** driver caused the VSCSI adapter to go offline and fail to recover. This update re-enables interrupts so that when the Virtual I/O Server is ready and sends the CRQ initialization request, it is properly received and processed.

BZ#710477

This update ensures that all remote ports are deleted when a Virtual I/O Server fails in a dual Virtual I/O Server multipath configuration, so that a path failover works as expected and the **ibmvfc** driver no longer becomes unresponsive. For a single path configuration, the remote ports go into a *devloss* state.

BZ#717742

Installation of HVM guests failed on AMD hosts. This update provides a number of patches which resolve this issue, and HVM guests can be installed on AMD hosts as expected.

BZ#710498

Using iSCSI offload resulted in EEH (Enhanced Error Handling) errors caused by missing programming of the page sizes on systems which do not use the 4K PAGE_SIZE. With this update, the underlying source code has been modified to address this issue, and EEH errors no longer occur when using iSCSI offload.

BZ#700546

File system corruption could occur on a file system with the qla2xxx driver due to missing block I/O back/front segment size setting. This update adds the block I/O back/front segment size setting, resolving this issue.

Enhancements:

BZ#696182, BZ#696182, BZ#707299

The **tg3** network driver has been updated to support the Broadcom 5720 Network Interface Controller. Additionally, the **tg3** network driver includes a number of fixes to support the Broadcom 5719 Network Interface Controller.

BZ#684842

The **mpt2sas** driver now allows customer specific display support.

BZ#689047

Support for DMI OEM flags to set **pci=bfsort** has been added.

BZ#651429

The **ipr** driver now supports the SAS VRAID capability on the new CRoC-based SAS adapters on IBM POWER7 systems.

BZ#684361

The AHCI driver has been updated to support for SATA RAID on future Intel chipsets.

BZ#570366

The **ixgbe** driver now provides support for PCIe AER (Advanced Error Reporting).

These updated kernel packages also upgrade a number of kernel device drivers. A list of these updated drivers can be found in the Red Hat Enterprise Linux 5.7 Release Notes.

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.

1.74.5. RHSA-2011:0927: Important kernel security and bug fix update

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.

This update fixes the following security issues:

* An integer overflow flaw in ib_uverbs_poll_cq() could allow a local, unprivileged user to cause a denial of service or escalate their privileges. (CVE-2010-4649, Important)

* A race condition in the way new InfiniBand connections were set up could allow a remote user to cause a denial of service. (CVE-2011-0695, Important)

* A flaw in the Stream Control Transmission Protocol (SCTP) implementation could allow a remote attacker to cause a denial of service if the sysctl "net.sctp.addip_enable" variable was turned on (it is off by default). (CVE-2011-1573, Important)

* Flaws in the AGPGART driver implementation when handling certain IOCTL commands could allow a local, unprivileged user to cause a denial of service or escalate their privileges. (CVE-2011-1745, CVE-2011-2022, Important)

* An integer overflow flaw in agp_allocate_memory() could allow a local, unprivileged user to cause a denial of service or escalate their privileges. (CVE-2011-1746, Important)

* A flaw allowed napi_reuse_skb() to be called on VLAN (virtual LAN) packets. An attacker on the local network could trigger this flaw by sending specially-crafted packets to a target system, possibly causing a denial of service. (CVE-2011-1576, Moderate)

* An integer signedness error in next_pidmap() could allow a local, unprivileged user to cause a denial of service. (CVE-2011-1593, Moderate)

* A flaw in the way the Xen hypervisor implementation handled CPUID instruction emulation during virtual machine exits could allow an unprivileged guest user to crash a guest. This only affects systems that have an Intel x86 processor with the Intel VT-x extension enabled. (CVE-2011-1936, Moderate)

* A flaw in inet_diag_bc_audit() could allow a local, unprivileged user to cause a denial of service (infinite loop). (CVE-2011-2213, Moderate)

* A missing initialization flaw in the XFS file system implementation could lead to an information leak. (CVE-2011-0711, Low)

* A flaw in ib_uverbs_poll_cq() could allow a local, unprivileged user to cause an information leak. (CVE-2011-1044, Low)

* A missing validation check was found in the signals implementation. A local, unprivileged user could use this flaw to send signals via the sigqueueinfo system call, with the si_code set to SI_TKILL and with spoofed process and user IDs, to other processes. Note: This flaw does not allow existing permission checks to be bypassed; signals can only be sent if your privileges allow you to already do so. (CVE-2011-1182, Low)

* A heap overflow flaw in the EFI GUID Partition Table (GPT) implementation could allow a local attacker to cause a denial of service by mounting a disk containing specially-crafted partition tables. (CVE-2011-1776, Low)

* Structure padding in two structures in the Bluetooth implementation was not initialized properly before being copied to user-space, possibly allowing local, unprivileged users to leak kernel stack memory to user-space. (CVE-2011-2492, Low)

Red Hat would like to thank Jens Kuehnel for reporting CVE-2011-0695; Vasiliy Kulikov for reporting CVE-2011-1745, CVE-2011-2022, and CVE-2011-1746; Ryan Sweat for reporting CVE-2011-1576;

Robert Swiecki for reporting CVE-2011-1593; Dan Rosenberg for reporting CVE-2011-2213 and CVE-2011-0711; Julien Tinnes of the Google Security Team for reporting CVE-2011-1182; Timo Warns for reporting CVE-2011-1776; and Marek Kroemeke and Filip Palian for reporting CVE-2011-2492.

This update also fixes several bugs and adds various enhancements. Documentation for these bug fixes and enhancements is available in the Red Hat Enterprise Linux 5.6 Technical Notes .

Users should upgrade to these updated packages, which contain backported patches to correct these issues, and fix the bugs noted in the Technical Notes. The system must be rebooted for this update to take effect.

1.74.6. RHSA-2011:0833: Important kernel security and bug fix update

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.

This update fixes the following security issues:

* A flaw in the dccp_rcv_state_process() function could allow a remote attacker to cause a denial of service, even when the socket was already closed. (CVE-2011-1093, Important)

* Multiple buffer overflow flaws were found in the Linux kernel's Management Module Support for Message Passing Technology (MPT) based controllers. A local, unprivileged user could use these flaws to cause a denial of service, an information leak, or escalate their privileges. (CVE-2011-1494, CVE-2011-1495, Important)

* A missing validation of a null-terminated string data structure element in the bnep_sock_ioctl() function could allow a local user to cause an information leak or a denial of service. (CVE-2011-1079, Moderate)

* Missing error checking in the way page tables were handled in the Xen hypervisor implementation could allow a privileged guest user to cause the host, and the guests, to lock up. (CVE-2011-1166, Moderate)

* A flaw was found in the way the Xen hypervisor implementation checked for the upper boundary when getting a new event channel port. A privileged guest user could use this flaw to cause a denial of service or escalate their privileges. (CVE-2011-1763, Moderate)

* The start_code and end_code values in "/proc/[pid]/stat" were not protected. In certain scenarios, this flaw could be used to defeat Address Space Layout Randomization (ASLR). (CVE-2011-0726, Low)

* A missing initialization flaw in the sco_sock_getsockopt() function could allow a local, unprivileged user to cause an information leak. (CVE-2011-1078, Low)

* A missing validation of a null-terminated string data structure element in the do_replace() function could allow a local user who has the CAP_NET_ADMIN capability to cause an information leak. (CVE-2011-1080, Low)

* A buffer overflow flaw in the DEC Alpha OSF partition implementation in the Linux kernel could allow a local attacker to cause an information leak by mounting a disk that contains specially-crafted partition tables. (CVE-2011-1163, Low)

* Missing validations of null-terminated string data structure elements in the do_replace(), compat_do_replace(), do_ipt_get_ctl(), do_ip6t_get_ctl(), and do_arpt_get_ctl() functions could allow a local user who has the CAP_NET_ADMIN capability to cause an information leak. (CVE-2011-1170, CVE-2011-1171, CVE-2011-1172, Low)

* A heap overflow flaw in the Linux kernel's EFI GUID Partition Table (GPT) implementation could allow a local attacker to cause a denial of service by mounting a disk that contains specially-crafted partition tables. (CVE-2011-1577, Low)

Red Hat would like to thank Dan Rosenberg for reporting CVE-2011-1494 and CVE-2011-1495; Vasiliy Kulikov for reporting CVE-2011-1079, CVE-2011-1078, CVE-2011-1080, CVE-2011-1170, CVE-2011-1171, and CVE-2011-1172; Kees Cook for reporting CVE-2011-0726; and Timo Warns for reporting CVE-2011-1163 and CVE-2011-1577.

This update also fixes several bugs and adds various enhancements. Documentation for these bug fixes and enhancements is available in the Red Hat Enterprise Linux 5.6 Technical Notes .

Users should upgrade to these updated packages, which contain backported patches to correct these issues, and fix the bugs noted in the Technical Notes. The system must be rebooted for this update to take effect.

1.74.7. RHSA-2011:0429: Important kernel security and bug fix update

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.

This update fixes the following security issues:

* A missing boundary check was found in the dvb_ca_ioctl() function in the Linux kernel's av7110 module. On systems that use old DVB cards that require the av7110 module, a local, unprivileged user could use this flaw to cause a denial of service or escalate their privileges. (CVE-2011-0521, Important)

* An inconsistency was found in the interaction between the Linux kernel's method for allocating NFSv4 (Network File System version 4) ACL data and the method by which it was freed. This inconsistency led to a kernel panic which could be triggered by a local, unprivileged user with files owned by said user on an NFSv4 share. (CVE-2011-1090, Moderate)

* A NULL pointer dereference flaw was found in the Generic Receive Offload (GRO) functionality in the Linux kernel's networking implementation. If both GRO and promiscuous mode were enabled on an interface in a virtual LAN (VLAN), it could result in a denial of service when a malformed VLAN frame is received on that interface. (CVE-2011-1478, Moderate)

* A missing security check in the Linux kernel's implementation of the install_special_mapping() function could allow a local, unprivileged user to bypass the mmap_min_addr protection mechanism. (CVE-2010-4346, Low)

* An information leak was found in the Linux kernel's task_show_regs() implementation. On IBM S/390 systems, a local, unprivileged user could use this flaw to read /proc/[PID]/status files, allowing them to discover the CPU register values of processes. (CVE-2011-0710, Low)

* A missing validation check was found in the Linux kernel's mac_partition() implementation, used for

supporting file systems created on Mac OS operating systems. A local attacker could use this flaw to cause a denial of service by mounting a disk that contains specially-crafted partitions. (CVE-2011-1010, Low)

Red Hat would like to thank Ryan Sweat for reporting CVE-2011-1478; Tavis Ormandy for reporting CVE-2010-4346; and Timo Warns for reporting CVE-2011-1010.

This update also fixes several bugs and adds various enhancements. Documentation for these bug fixes and enhancements is available in the Red Hat Enterprise Linux 5.6 Technical Notes .

Users should upgrade to these updated packages, which contain backported patches to correct these issues, and fix the bugs noted in the Technical Notes. The system must be rebooted for this update to take effect.

1.74.8. RHSA-2011:0303: Moderate kernel security and bug fix update

Updated kernel packages that fix three 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 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 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 Linux kernel's garbage collector for AF_UNIX sockets. A local, unprivileged user could use this flaw to trigger a denial of service (out-of-memory condition). (CVE-2010-4249, Moderate)

* A flaw was found in the Linux kernel's networking subsystem. If the number of packets received exceeded the receiver's buffer limit, they were queued in a backlog, consuming memory, instead of being discarded. A remote attacker could abuse this flaw to cause a denial of service (out-of-memory condition). (CVE-2010-4251, Moderate)

* A missing initialization flaw was found in the ethtool_get_regs() function in the Linux kernel's ethtool IOCTL handler. A local user who has the CAP_NET_ADMIN capability could use this flaw to cause an information leak. (CVE-2010-4655, Low)

Red Hat would like to thank Vegard Nossum for reporting CVE-2010-4249, and Kees Cook for reporting CVE-2010-4655.

This update also fixes several bugs and adds various enhancements. Documentation for these bug fixes and enhancements is available in the Red Hat Enterprise Linux 5.6 Technical Notes .

Users should upgrade to these updated packages, which contain backported patches to correct these issues, and fix the bugs noted in the Technical Notes. The system must be rebooted for this update to take effect.

1.74.9. RHSA-2011:0163: Important kernel security and bug fix update

Updated kernel packages that fix one security issue and three 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. 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 kernel packages contain the Linux kernel, the core of any Linux operating system.

This update fixes the following security issue:

* A flaw was found in the sctp_icmp_proto_unreachable() function in the Linux kernel's Stream Control Transmission Protocol (SCTP) implementation. A remote attacker could use this flaw to cause a denial of service. (CVE-2010-4526, Important)

This update also fixes the following bugs:

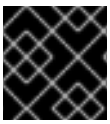
* Due to an off-by-one error, gfs2_grow failed to take the very last "rgrp" parameter into account when adding up the new free space. With this update, the GFS2 kernel properly counts all the new resource groups and fixes the "statfs" file correctly. (BZ#666792)

* Prior to this update, a multi-threaded application, which invoked popen(3) internally, could cause a thread stall by FILE lock corruption. The application program waited for a FILE lock in glibc, but the lock seemed to be corrupted, which was caused by a race condition in the COW (Copy On Write) logic. With this update, the race condition was corrected and FILE lock corruption no longer occurs. (BZ#667050)

* If an error occurred during I/O, the SCSI driver reset the "megaraid_sas" controller to restore it to normal state. However, on Red Hat Enterprise Linux 5, the waiting time to allow a full reset completion for the "megaraid_sas" controller was too short. The driver incorrectly recognized the controller as stalled, and, as a result, the system stalled as well. With this update, more time is given to the controller to properly restart, thus, the controller operates as expected after being reset. (BZ#667141)

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.

1.74.10. RHSA-2011:1386: Important: kernel security, bug fix, and enhancement update



IMPORTANT

This update has already been released as the security errata RHSA-2011:1386.

Updated kernel packages that fix multiple security issues, several bugs, 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 important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links after each description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security fixes

The maximum file offset handling for ext4 file systems could allow a local, unprivileged user to cause a denial of service. (CVE-2011-2695, Important)

IPv6 fragment identification value generation could allow a remote attacker to disrupt a target system's networking, preventing legitimate users from accessing its services. (CVE-2011-2699, Important)

A malicious CIFS (Common Internet File System) server could send a specially-crafted response to a directory read request that would result in a denial of service or privilege escalation on a system that has a CIFS share mounted. (CVE-2011-3191, Important)

A local attacker could use mount.ecryptfs_private to mount (and then access) a directory they would otherwise not have access to. Note: To correct this issue, the RHSA-2011:1241 ecryptfs-utils update must also be installed. (CVE-2011-1833, Moderate)

A flaw in the taskstats subsystem could allow a local, unprivileged user to cause excessive CPU time and memory use. (CVE-2011-2484, Moderate)

Mapping expansion handling could allow a local, unprivileged user to cause a denial of service. (CVE-2011-2496, Moderate)

GRO (Generic Receive Offload) fields could be left in an inconsistent state. An attacker on the local network could use this flaw to cause a denial of service. GRO is enabled by default in all network drivers that support it. (CVE-2011-2723, Moderate)

RHSA-2011:1065 introduced a regression in the Ethernet bridge implementation. If a system had an interface in a bridge, and an attacker on the local network could send packets to that interface, they could cause a denial of service on that system. Xen hypervisor and KVM (Kernel-based Virtual Machine) hosts often deploy bridge interfaces. (CVE-2011-2942, Moderate)

A flaw in the Xen hypervisor IOMMU error handling implementation could allow a privileged guest user, within a guest operating system that has direct control of a PCI device, to cause performance degradation on the host and possibly cause it to hang. (CVE-2011-3131, Moderate)

IPv4 and IPv6 protocol sequence number and fragment ID generation could allow a man-in-the-middle attacker to inject packets and possibly hijack connections. Protocol sequence number and fragment IDs are now more random. (CVE-2011-3188, Moderate)

A flaw in the kernel's clock implementation could allow a local, unprivileged user to cause a denial of service. (CVE-2011-3209, Moderate)

Non-member VLAN (virtual LAN) packet handling for interfaces in promiscuous mode and also using the be2net driver could allow an attacker on the local network to cause a denial of service. (CVE-2011-3347, Moderate)

A flaw in the auerswald USB driver could allow a local, unprivileged user to cause a denial of service or escalate their privileges by inserting a specially-crafted USB device. (CVE-2009-4067, Low)

A flaw in the Trusted Platform Module (TPM) implementation could allow a local, unprivileged user to leak information to user space. (CVE-2011-1160, Low)

A local, unprivileged user could possibly mount a CIFS share that requires authentication without knowing the correct password if the mount was already mounted by another local user. (CVE-2011-1585, Low)

Red Hat would like to thank Fernando Gont for reporting CVE-2011-2699; Darren Lavender for reporting CVE-2011-3191; the Ubuntu Security Team for reporting CVE-2011-1833; Vasiliy Kulikov of Openwall for reporting CVE-2011-2484; Robert Swiecki for reporting CVE-2011-2496; Brent Meshier for reporting CVE-2011-2723; Dan Kaminsky for reporting CVE-2011-3188; Yasuaki Ishimatsu for reporting CVE-2011-3209; Somnath Kotur for reporting CVE-2011-3347; Rafael Dominguez Vega for

reporting CVE-2009-4067; and Peter Huewe for reporting CVE-2011-1160. The Ubuntu Security Team acknowledges Vasiliy Kulikov of Openwall and Dan Rosenberg as the original reporters of CVE-2011-1833.

Bug Fixes

BZ#739823

A previously applied patch to help clean-up a failed **nmi_watchdog** check by disabling various registers caused single-vcpu Xen HVM guests to become unresponsive during boot when the host CPU was an Intel Xeon Processor E5405 or an Intel Xeon Processor E5420, and the VM configuration did not have the ***apic = 1*** parameter set. With this update, **NMI_NONE** is the default watchdog on AMD64 HVM guests, thus, fixing this issue.

BZ#730686

A previously introduced patch forced the **->flush** and **->fsync** operations to wait on all WRITE and COMMIT remote procedure calls (RPC) to complete to ensure that those RPCs were completed before returning from **fsync()** or **close()**. As a consequence, all WRITEs issued by **nfs_flush_list** were serialized and caused a performance regression on NFS clients. This update changes **nfs_flush_one** and **nfs_flush_multi** to not wait for WRITEs issued when the ***FLUSH_SYNC*** parameter is set, resolving performance issues on NFS clients.

BZ#733665

When setting the value in the **/proc/sys/vm/dirty_writeback_centisecs** file via **echo**, the actual saved value was always one less than the given value (for example, setting 500 resulted in 499 being set). This update fixes this off-by-one error, and values in **/proc/sys/vm/dirty_writeback_centisecs** are now correctly set.

BZ#732775

When reading a file from a subdirectory in **/proc/bus/pci/** while hot-unplugging the device related to that file, the system would crash. With this update, the kernel correctly handles the simultaneous removal of a device, and access to the representation of that device in the **proc** file system.

BZ#738389

Prior to this update, MTU was constrained to 1500 unless Scatter/Gather I/O (SG) was supported by the NIC; in the case of netback, this would mean unless SG was supported by the front-end. Because the hotplugging scripts ran before features have been negotiated with the front-end, at that point SG would still be disabled, breaking anything using larger MTUs, (for example, cluster communication using that NIC). This update inverts the behavior and assumes SG to be present until negotiations prove otherwise (in such a case, MTU is automatically reduced).

BZ#734157

A previously applied patch introduced a regression for 3rd party file systems that do not set the ***FS_HAS_IODONE2*** flag, specifically, the Oracle Cluster File System 2 (OCFS2). The patch removed a call to the **aio_complete** function, resulting in no completion events being processed, causing userspace applications to become unresponsive. This update reintroduces the **aio_complete** function call, fixing this issue.

BZ#732946

This update fixes a race between TX and MCC events where an MCC event could kill a NAPI schedule by a succeeding TX event, which resulted in network transfer pauses.

BZ#730685

Previously, when the Xen Hypervisor split a 2 MB page into 4 KB pages, it linked the new page from the PDE (Page Directory Entry) before it filled entries of the page with appropriate data. Consequently, when doing a live migration with EPT (Extended Page Tables) enabled on a non-idle guest running with more than two virtual CPUs, the guest often terminated unexpectedly. With this update, the Xen Hypervisor prepares the page table entry first, and then links it in, fixing this bug.

BZ#730682

This update adds a missing patch that enables WOL (Wake-on-LAN) on the second port of a Intel Ethernet Server Adapter I350.

BZ#736275

Kernel panic occurred on a Red Hat Enterprise Linux 5.7 QLogic FCoE host during I/O operations with fabric faults due to a NULL ***fcport*** object dereference in the **qla24xx_queuecommand** function. This update adds a check that returns **DID_NO_CONNECT** if the ***fcport*** object is NULL.

BZ#732945

Packet statistics in **/proc/net/dev** occasionally jumped backwards. This was because the **cat /proc/net/dev** command was processed while the loop updating the counter was running, sometimes resulting in partially updated counter (causing the statistics to be incorrect). This update fixes this bug by using a temporary variable while summing up all the RX queues, and only then updating the **/proc/net/dev** statistics, making the whole operation atomic. Additionally, this update provides a patch that fixes a problem with the 16-bit RX dropped packets HW counter by maintaining a 32-bit accumulator in the driver to prevent frequent wraparound.

BZ#734772

Prior to this update, the **nosharecache** NFS mount option was not always honored. If two mount locations specified this option, the behavior would be the same as if the option was not specified. This was because of missing checks that enforced this option. This update adds the missing checks, resolving this issue.

BZ#728521

When kdump was triggered under a heavy load, the system became unresponsive and failed to capture a crash dump. This update fixes interrupt handling for kdump so that kdump successfully captures a crash dump while under a heavy load.

BZ#732440

Previously, configurations where Max BW was set to 0 produced the following message:

```
Illegal configuration detected for Max BW - using 100 instead.
```

With this update, such message is produced only when debugging is enabled, and such configuration is no longer called *Illegal*.

BZ#733152

If the **be2net** driver could not allocate new SKBs in the RX completion handler, it returned messages to the console and dropped packets. With this update, the driver increases the **netdevice** ***rx_dropped*** counter instead, and no longer produces messages in the console.

BZ#734761

If iSCSI was not supported on a **bnx2** device, the **bnx2_cnic_probe()** function returned NULL and the **cnic** device was not be visible to **bnx2i**. This prevented **bnx2i** from registering and then unregistering during **cnic_start()** and caused the following warning message to appear:

```
bnx2 0003:01:00.1: eth1: Failed waiting for ULP up call to complete
```

BZ#737475

Prior to this update, failures to bring up the Broadcom BCM57710 Ethernet Controller occurred and the following error messages:

```
eth0: Something bad had happen! Aii!
[bnx2x_release_hw_lock:1536(eth0)]Releasing a lock on resource 8
eth0: Recovery flow hasn't been properly completed yet. Try again later.
If u
still see this message after a few retries then power cycle is required.
```

With this update, the underlying source code has been modified to address this issue, and the Broadcom BCM57710 Ethernet Controller no longer fails to start.

BZ#738392

This update introduces support for jumbo frames in the Xen networking backend. However, old guests will still revert to a 1500-byte MTU after migration. This update also changes how the guest will probe the backend's Scatter/Gather I/O functionality. As long as a recent enough kernel is installed in the destination host, this will ensure that the guest will keep a large MTU even after migration.

BZ#736742

Previously, the **inet6_sk_generic()** function was using the ***obj_size*** variable to compute the address of its inner structure, causing memory corruption. With this update, the **sk_alloc_size()** is called every time there is a request for allocation, and memory corruption no longer occurs.

BZ#728518

Prior to this update, Xen did not implement certain ALU opcodes. As a result, when a driver used the missing opcodes on memory-mapped I/O areas, it caused the guest to crash. This update adds all the missing opcodes. In particular, this fixes a BSOD crash from the Windows **e1000** driver.

Enhancements

BZ#732377

With this update, the JSM driver has been updated to support the Bell2 (with PLX chip) 2-port adapter on IBM POWER7 systems. Additionally, EEH support has been added to JSM driver.

Users should upgrade to these updated packages, which contain backported patches to correct these issues and add this enhancement. The system must be rebooted for this update to take effect.

1.75. KEXEC-TOOLS

1.75.1. RHBA-2011:0382: kexec-tools bug fix update

An updated kexec-tools package that fixes one bug is now available for Red Hat Enterprise Linux 5 Extended Update Support.

The kexec fastboot mechanism allows booting a Linux kernel from the context of an already running kernel. The kexec-tools package provides the /sbin/kexec binary and ancillary utilities that form the user-space component of the kernel's kexec feature.

This update fixes the following bug:

* On certain hardware, the kexec kernel incorrectly attempted to use a reserved memory range, and failed to boot with an error. This update adapts the underlying source code to determine the size of a backup region dynamically. As a result, kexec no longer attempts to use the reserved memory range, and boots as expected. (BZ#682085)

All users of kexec-tools are advised to upgrade to this updated package, which fixes this bug.

1.75.2. RHBA-2011:0505: kexec-tools bug fix update

An updated kexec-tools package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The kexec fastboot mechanism allows booting a Linux kernel from the context of an already running kernel. The kexec-tools package provides the /sbin/kexec binary and ancillary utilities that form the user-space component of the kernel's kexec feature.

This update fixes the following bug:

* On x86 systems with a Physical Address Extension (PAE) kernel, the previous version of kexec-tools incorrectly attempted to use a reserved memory range and failed to create a valid core dump. This rendered the crash utility unable to read vmalloc addresses, and any attempt to analyze such a dump file caused the utility to display the following message:

WARNING: cannot access vmalloc'd module memory

This update applies a patch that prevents kexec-tools from incorrectly accessing a reserved memory range. Now, kexec-tools can generate core dump files that the crash utility can handle. (BZ#696547)

All users of kexec-tools are advised to upgrade to this updated package, which fixes this bug.

1.75.3. RHEA-2011:0146: kexec-tools enhancement update

An updated kexec-tools package that adds one enhancement is now available for Red Hat Enterprise Linux 5.

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.

This update adds the following enhancement:

* Red Hat Enterprise Linux 5 now fully supports the ext4 filesystem, but kdump fails to dump the vmcore on ext4 file systems. This update adds support to the ext4 file system so that users can dump the vmcore to an ext4 filesystem.

All users are advised to upgrade to this updated kexec-tools package, which adds this enhancement. (BZ#667966)

1.76. KRB5

1.76.1. RHSA-2011:0199: Important krb5 security update

Updated krb5 packages that fix two 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.

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).

A NULL pointer dereference flaw was found in the way the MIT Kerberos KDC processed principal names that were not null terminated, when the KDC was configured to use an LDAP back end. A remote attacker could use this flaw to crash the KDC via a specially-crafted request. (CVE-2011-0282)

A denial of service flaw was found in the way the MIT Kerberos KDC processed certain principal names when the KDC was configured to use an LDAP back end. A remote attacker could use this flaw to cause the KDC to hang via a specially-crafted request. (CVE-2011-0281)

Red Hat would like to thank the MIT Kerberos Team for reporting these issues. Upstream acknowledges Kevin Longfellow of Oracle Corporation as the original reporter of the CVE-2011-0281 issue.

All krb5 users should upgrade to these updated packages, which contain a backported patch to correct these issues. After installing the updated packages, the krb5kdc daemon will be restarted automatically.

1.76.2. RHBA-2011:1031: krb5 bug fix and enhancement update

Updated krb5 packages that fix multiple bugs and add one enhancement are now available for Red Hat Enterprise Linux 5.

Kerberos is a network authentication system which allows clients and servers to authenticate to each other with the help of a trusted third party, a KDC.

This update fixes the following bugs:

* Prior to this update,the lock of the realm database could, under certain circumstances, not be released. Due to this problem, the lock could not be acquired until the clearing process was stopped or restarted. With this update, the realm database is successfully locked. (BZ#586032)

* Prior to this update,the Kerberos-aware FTP server did not parse the "restrict" keyword correctly when it was used in /etc/ftpusers. This update modifies the code so that the server parses the "restrict" keyword correctly. (BZ#644215)

* Prior to this update,the Kerberos-aware FTP client did not correctly display the size of a transferred file on 32-bit systems if the size of the file exceeded 4GB. This update modifies the type of the variable used to track the number of bytes transferred. (BZ#648404)

* Prior to this update, the client libraries failed, under certain circumstances, to parse an error reply message from the server when trying to change passwords. With this update, the client library can parse the message and correctly returns the reported error to its caller. (BZ#658871)

* Prior to this update, Kerberos-aware servers leaked memory when replay caching was disabled. This update modifies the code so that no more memory leaks occur. (BZ#678205)

* Prior to this update, the SELinux label was not maintained for replay cache files when expired entries were expunged. This update maintains the reply cache files in such a case. (BZ#712453)

This update also adds the following enhancement:

* Prior to this update, the Kerberos-aware FTP client was not able to parse user commands if the length of the command exceeded the limit of 500 characters. This update allows for the Kerberos-aware FTP client to parse user commands without character limit. (BZ#665833)

All Kerberos users are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

1.76.3. RHBA-2011:0904: krb5 bug fix update

Updated krb5 packages that fix a bug are now available for Red Hat Enterprise Linux 5.

Kerberos is a network authentication system which allows clients and servers to authenticate to each other with the help of a trusted third party, a KDC (Key Distribution Center).

This update fixes the following bug:

* When expired entries are being expunged from cache, Kerberos creates a temporary file, copies valid entries into it and then renames it back to set it as a new cache file. Prior to this update, the SELinux label was not set correctly for the temporary file. Subsequently, user identities could not be properly verified. With this update, a newer version of the patch addressing this issue has been provided, the temporary file now gets the correct SELinux label and applications that modify the replay cache file continue to work properly in the described scenario. (BZ#714188)

Users of krb5 are advised to upgrade to these updated packages, which fix this bug.

1.77. KSH

1.77.1. RHBA-2011:0304: ksh bug fix update

An updated ksh package that fixes multiple bugs is now available for Red Hat Enterprise Linux 5.

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 update fixes the following bugs:

* Due to a memory leak in the ksh executable, the performance of long running scripts could decrease significantly over the time. With this update, the underlying source code has been modified to prevent this memory leak, and the execution of long running scripts is no longer slowed down. (BZ#674552)

* When a ksh script contained the "trap" command to capture a "SIGPIPE" signal, sending this signal by using the built-in "echo" command could cause its output to be incorrectly added to the redirected output of an external command. This error has been fixed, and ksh now flushes the output buffer before redirecting output streams. (BZ#675128)

* Due to incorrect signal handling, receiving a signal while still processing the same one caused ksh to terminate unexpectedly with a segmentation fault. With this update, the subsequent signals are deferred until the current one is processed, and ksh no longer crashes. (BZ#675130)

* Previously, assigning a value to an array variable during the execution of the "typeset" command could cause the shell to terminate unexpectedly with a segmentation fault. This update corrects the array handling in this command, and ksh no longer crashes. (BZ#675135)

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

1.77.2. RHBA-2011:0385: ksh bug fix update

An updated ksh package that fixes various bugs is now available for Red Hat Enterprise Linux 5.

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 update fixes the following bugs:

* The KornShell's "IFS" variable contains a list of field separators and is used to separate the results of command substitution, parameter expansion, or separate fields with the "read" built-in command. Previously, ksh did not protect this variable from being freed. Consequent to this, when a user attempted to unset the "IFS" variable from within a function, ksh terminated unexpectedly with a segmentation fault. With this update, an upstream patch has been applied to address this issue, and using the "unset IFS" command inside a function body no longer causes ksh to crash. (BZ#684829)

* When a ksh script created a file and immediately opened it after the creation, the operation failed. This happened because the created file, in some cases, did not exist yet. With this update, this race condition has been fixed and once a file is created, it is immediately available for any following commands. (BZ#684831)

* Prior to this update, ksh did not close a file containing an auto-loaded function definition. After loading several functions, ksh could have easily exceeded the system's limit on the number of open files. With this update, files containing auto-loaded functions are properly closed, thus, the number of opened files no longer increases with usage. (BZ#684832)

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

1.77.3. RHBA-2011:0513: ksh bug fix update

An updated ksh package that fixes one bug is now available for Red Hat Enterprise Linux 5.

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 update fixes the following bug:

* When running a script, the previous version of ksh could incorrectly consider the "eval" command to be the last in the script, and did not run it in a separate process. Consequent to this, using "eval" or executing commands from another file (that is, by using the "." built-in command) may have prevented ksh from executing any subsequent commands. With this update, the underlying source code has been adapted to determine whether a script contains other commands, and perform the selected action in a separate process if it does. As a result, ksh now executes all commands in a script as expected. (BZ#702364)

All users of ksh are advised to upgrade to this updated package, which fixes this bug.

1.77.4. RHBA-2011:0939: ksh bug fix update

An updated ksh package that fixes one bug is now available for Red Hat Enterprise Linux 5.

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 update fixes the following bug:

* Previously, ksh treated an array declaration as a definition. Consequently, the array contained one element after the declaration. This bug has been fixed, and now an array is correctly reported as empty after a declaration. (BZ#716375)

All users of ksh are advised to upgrade to this updated package, which fixes this bug.

1.78. KVM

1.78.1. RHBA-2011:1068: kvm bug fix update

Updated kvm packages that fix various bugs are now available for Red Hat Enterprise Linux 5.

IMPORTANT

This update was released as errata RHBA-2011:1068 — kvm bug fix update.

KVM (Kernel-based Virtual Machine) is a full virtualization solution for Linux on hardware containing virtualization extensions (i.e. nearly all modern hardware). It consists of a loadable kernel module, **`kvm.ko`**, that provides the core virtualization infrastructure and a processor specific module, **`kvm-intel.ko`** or **`kvm-amd.ko`**.

Bug Fixes:

BZ#561224

When the Sandra multi-media benchmark utility was run on a Windows guest, the guest terminated unexpectedly when the utility tried to access the Model Specific Register 0x480 (IA32_VMX_BASIC). A patch has been provided to address this issue and the benchmark utility no longer causes a Windows guest to crash.

BZ#666225, BZ#693918

When a migration was attempted during the early boot stage in a virtual machine running Windows XP, the virtual machine failed to boot correctly. This bug has been fixed, and the virtual machine now boots properly in the described scenario.

BZ#713389

When a host with a floppy drive attached and Red Hat Enterprise Linux 5.7 installed was being migrated to another host with kernel version 2.6.18-238.14.1 installed, the migration process failed and the host was left in a stopped state. A patch has been provided to address this issue and the migration now finishes successfully in the described scenario.

BZ#713392

Due to a regression, when the values for maximum downtime or maximum speed were increased during a migration, the guests experienced heavy stalls and the migration did not finish in a

reasonable time. With this update, a patch has been provided and the migration process finishes successfully in the described scenario.

BZ#508949

When an iSCSI server was configured and the block device was shared on a host, if a guest on another host performed a write operation on the shared device and the iSCSI server was restarted, the standard output of the QEMU monitor on the source host was flooded with redundant error messages. With this update, calls to write out these messages have been removed from the code, thus fixing this bug.

BZ#641854

Previously, when a CD image with a read-only flag set was ejected from a drive on a guest, the read-only flag was preserved. Consequently, the image could not be re-attached to the drive. A patch has been provided to address this issue, and the read-write flag is now set correctly when an image is ejected from a drive, allowing CD images to be changed on-the-fly.

BZ#644706

Previously, the QEMU monitor used an incorrect handler to process passwords to encrypted images. Consequently, the monitor became unresponsive on the first command when attempting to start a guest with an encrypted **qcow2** (QEMU Copy-on-Write) image. With this update, the command handler and the password handler are used properly, and the guest now starts successfully in the described scenario.

BZ#644793

In hot plug mode, when a PCI device was being attached to a QEMU guest with the **-no-kvm** command line option, the **qemu-kvm** utility terminated with a segmentation fault. This bug has been fixed, and **qemu-kvm** now exits properly and returns appropriate error messages in the described scenario.

BZ#581555

When the **cont** command of the QEMU monitor was used to restore a domain saved to a file via the **virsh** utility, if an incoming migration had been specified for the virtual machine, **cont** sometimes took effect before the migration was complete. As a consequence, the restore process or the migration sometimes failed. This bug has been fixed, and now the **cont** command is only accepted after the incoming migration has successfully finished.

BZ#652135

Due to flaws in the IDE CD-ROM emulation, the guest kernel and the **anaconda** installer sometimes failed to recognize the installation media after the optional testing of installation media had been made. Consequently, the installation process became unresponsive and could not continue. With this update, a memory leak in the **bdrv_close()** function has been fixed, the installation process no longer gets stuck and the retry function can now be properly used if the installation medium is not recognized the first time.

BZ#657149

When a **system_reset** signal was sent to a guest with a pass-through NIC (Network Interface Card) attached, a kernel panic occurred in the guest. This bug has been fixed, and the guest now reboots properly in the described scenario.

BZ#659172

When the *CHAOS-Concurrent Hardware And OS test*job was run in the WHQL (Windows Hardware

Quality Labs) test environment on a Windows guest, the `run pwrtest` child job failed even though the main *CHAOS* job passed. This bug has been fixed in the KVM BIOS, and the `run pwrtest` job now passes successfully in the described scenario.

BZ#665023

The QEMU emulator did not enqueue mouse events; it simply records the latest mouse state. Prior to this update, double click or dragging mouse events were sometimes lost, especially on high-latency connections. Now, the code for mouse descriptors has been fixed, and lost mouse events occur much less frequently.

Users of kvm are advised to upgrade to these updated packages, which fix these bugs.

1.78.2. RHBA-2011:0499: kvm bug fix update

Updated kvm packages that fix one bug are now available for Red Hat Enterprise Linux 5.

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.

This update fixes the following bug:

* Due to a regression introduced in Red Hat Enterprise Linux 5.6, duplicate pages may have been transferred during a live migration of a KVM virtual machine. Consequent to this, when a system was under heavy load, such a migration may have failed to complete in some scenarios. This update applies a patch that reverts this regression. As a result, the live migration is now more efficient and no longer fails to complete under heavy load. (BZ#696155)

All users of kvm are advised to upgrade to these updated packages, which fix this bug. Note that the procedure in the Solution section must be performed before this update will take effect.

1.79. LAPACK

1.79.1. RHBA-2011:0442: lapack bug fix update

Updated lapack packages that fix one bug are now available for Red Hat Enterprise Linux 5.

LAPACK (Linear Algebra PACKage) is a standard library for numerical linear algebra written in FORTRAN 77. It provides routines for solving systems of simultaneous linear equations, least-squares solutions of linear systems of equations, eigenvalue problems, and singular value problems.

This update fixes the following bug:

* Prior to this update, the "DLALSD" function incorrectly modified the value of the "RCOND" argument. Consequent to this, an attempt to call this function with a literal value such as "-1.D0" as the "RCOND" argument caused the calling program to terminate unexpectedly with a segmentation fault. With this update, a patch has been applied to prevent "DLALSD" from modifying the value of "RCOND", and the use of a literal value no longer causes the program to crash. (BZ#608039)

All users of lapack are advised to upgrade to these updated packages, which fix this bug.

1.80. LIBDHCP

1.80.1. RHBA-2011:1027: libdhcp bug fix update

Updated libdhcp packages that fix one bug are now available for Red Hat Enterprise Linux 5.

libdhcp enables programs to invoke and control the Dynamic Host Configuration Protocol (DHCP) clients: the Internet Software Consortium (ISC) IPv4 DHCP client library, libdhcp4client, and the IPv6 DHCPv6 client library, libdhcp6client.

This update fixes the following bug:

* Prior to this update, the libdhcp4client client library did not support IP over InfiniBand (IPoIB) devices. With this update, libdhcp is rebuilt against the latest libdhcp4client packages, which add support for IPoIB devices. (BZ#694570)

All users of libdhcp are advised to upgrade to these updated packages, which fix this bug.

1.81. LIBMLX4

1.81.1. RHBA-2011:1057: libmlx4 enhancement update

Updated libmlx4 packages that add one enhancement are now available for Red Hat Enterprise Linux 5.

libmlx4 is the hardware driver library for Mellanox ConnectX architecture devices for use with the libibverbs user space verbs access library.

This update adds the following enhancement:

* This update adds new PCI IDs to the library to allow libmlx4 to work with recently released devices. (BZ#670887)

Users who require Mellanox InfiniBand hardware are advised to upgrade to these updated packages, which add this enhancement.

1.82. LIBTDB

1.82.1. RHBA-2011:1050: libtdb bug fix update

Updated libtdb packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The libtdb library implements the small Trivial Database (TDB).

This update fixes the following bug:

* Prior to this update, the built-in logic in TDB for automatic resizing did not allow for databases with very large records. Due to this issue, the database allocated far more memory than required when a large record was entered into the database, which forced a resize. With this update, the size of the records are taken into consideration when resizing the database. Now, only the required amount of memory is allocated. (BZ#693785)

All users of libtdb are advised to upgrade to these updated packages, which fix this bug.

1.83. LIBTIFF

1.83.1. RHSA-2011:0392: Important libtiff security and bug fix update

Updated libtiff packages that fix one security issue and one bug are now available for Red Hat Enterprise Linux 4, 5, and 6.

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.

The libtiff packages contain a library of functions for manipulating Tagged Image File Format (TIFF) files.

A heap-based buffer overflow flaw was found in the way libtiff processed certain TIFF files encoded with a 4-bit run-length encoding scheme from ThunderScan. An attacker could use this flaw to create a specially-crafted TIFF file that, when opened, would cause an application linked against libtiff to crash or, possibly, execute arbitrary code. (CVE-2011-1167)

This update also fixes the following bug:

* The RHSA-2011:0318 libtiff update introduced a regression that prevented certain TIFF Internet Fax image files, compressed with the CCITT Group 4 compression algorithm, from being read. (BZ#688825)

All libtiff users should upgrade to these updated packages, which contain a backported patch to resolve these issues. All running applications linked against libtiff must be restarted for this update to take effect.

1.83.2. RHSA-2011:0318: Important libtiff security update

Updated libtiff packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

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.

The libtiff packages contain a library of functions for manipulating Tagged Image File Format (TIFF) files.

A heap-based buffer overflow flaw was found in the way libtiff processed certain TIFF Internet Fax image files, compressed with the CCITT Group 4 compression algorithm. An attacker could use this flaw to create a specially-crafted TIFF file that, when opened, would cause an application linked against libtiff to crash or, possibly, execute arbitrary code. (CVE-2011-0192)

Red Hat would like to thank Apple Product Security for reporting this issue.

All libtiff users should upgrade to these updated packages, which contain a backported patch to resolve this issue. All running applications linked against libtiff must be restarted for this update to take effect.

1.84. LIBUSER

1.84.1. RHSA-2011:0170: Moderate libuser security update

Updated libuser packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

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 libuser library implements a standardized interface for manipulating and administering user and group accounts. Sample applications that are modeled after applications from the shadow password suite (shadow-utils) are included in these packages.

It was discovered that libuser did not set the password entry correctly when creating LDAP (Lightweight Directory Access Protocol) users. If an administrator did not assign a password to an LDAP based user account, either at account creation with luseradd, or with lpasswd after account creation, an attacker could use this flaw to log into that account with a default password string that should have been rejected. (CVE-2011-0002)

Note: LDAP administrators that have used libuser tools to add users should check existing user accounts for plain text passwords, and reset them as necessary.

Users of libuser should upgrade to these updated packages, which contain a backported patch to correct this issue.

1.85. LIBVIRT

1.85.1. RHSA-2011:0478: Moderate libvirt security update

Updated libvirt 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 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 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.

A flaw was found in the way libvirtd handled error reporting for concurrent connections. A remote attacker able to establish read-only connections to libvirtd on a server could use this flaw to crash libvirtd. (CVE-2011-1486)

All libvirt users are advised to upgrade to these updated packages, which contain backported patches to resolve this issue. After installing the updated packages, libvirtd must be restarted ("service libvirtd restart") for this update to take effect.

1.85.2. RHSA-2011:0391: Important libvirt security update

Updated libvirt packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

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.

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.

It was found that several libvirt API calls did not honor the read-only permission for connections. A local attacker able to establish a read-only connection to libvirtd on a server could use this flaw to execute commands that should be restricted to read-write connections, possibly leading to a denial of service or privilege escalation. (CVE-2011-1146)

Note: Previously, using rpmbuild without the '--define "rhel 5"' option to build the libvirt source RPM on Red Hat Enterprise Linux 5 failed with a "Failed build dependencies" error for the device-mapper-devel package, as this -devel sub-package is not available on Red Hat Enterprise Linux 5. With this update, the -devel sub-package is no longer checked by default as a dependency when building on Red Hat Enterprise Linux 5, allowing the libvirt source RPM to build as expected.

All libvirt users are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing the updated packages, libvirtd must be restarted ("service libvirtd restart") for this update to take effect.

1.85.3. RHSA-2011:1019: Moderate libvirt security, bug fix, and enhancement update

Updated libvirt packages that fix one security issue, several bugs and add various 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.

The libvirt library is a C API for managing and interacting with the virtualization capabilities of Linux and other operating systems.

An integer overflow flaw was found in libvirtd's RPC call handling. An attacker able to establish read-only connections to libvirtd could trigger this flaw by calling virDomainGetVcpus() with specially-crafted parameters, causing libvirtd to crash. (CVE-2011-2511)

This update fixes the following bugs:

* libvirt was rebased from version 0.6.3 to version 0.8.2 in Red Hat Enterprise Linux 5.6. A code audit found a minor API change that effected error messages seen by libvirt 0.8.2 clients talking to libvirt 0.7.1 – 0.7.7 (0.7.x) servers. A libvirt 0.7.x server could send VIR_ERR_BUILD_FIREWALL errors where a libvirt 0.8.2 client expected VIR_ERR_CONFIG_UNSUPPORTED errors. In other circumstances, a libvirt 0.8.2 client saw a "Timed out during operation" message where it should see an "Invalid network filter" error. This update adds a backported patch that allows libvirt 0.8.2 clients to interoperate with the API as used by libvirt 0.7.x servers, ensuring correct error messages are sent. (BZ#665075)

* libvirt could crash if the maximum number of open file descriptors (_SC_OPEN_MAX) grew larger than the FD_SETSIZE value because it accessed file descriptors outside the bounds of the set. With this update the maximum number of open file descriptors can no longer grow larger than the FD_SETSIZE value. (BZ#665549)

* A libvirt race condition was found. An array in the libvirt event handlers was accessed with a lock temporarily released. In rare cases, if one thread attempted to access this array but a second thread reallocated the array before the first thread reacquired a lock, it could lead to the first thread attempting to access freed memory, potentially causing libvirt to crash. With this update libvirt no longer refers to the old array and, consequently, behaves as expected. (BZ#671569)

* Guests connected to a passthrough NIC would kernel panic if a system_reset signal was sent through

the QEMU monitor. With this update you can reset such guests as expected. (BZ#689880)

* When using the Xen kernel, the rpmbuild command failed on the xencapstest test. With this update you can run rpmbuild successfully when using the Xen kernel. (BZ#690459)

* When a disk was hot unplugged, "ret >= 0" was passed to the qemuAuditDisk calls in disk hotunplug operations before ret was, in fact, set to 0. As well, the error path jumped to the "cleanup" label prematurely. As a consequence, hotunplug failures were not audited and hotunplug successes were audited as failures. This was corrected and hot unplugging checks now behave as expected. (BZ#710151)

* A conflict existed between filter update locking sequences and virtual machine startup locking sequences. When a filter update occurred on one or more virtual machines, a deadlock could consequently occur if a virtual machine referencing a filter was started. This update changes and makes more flexible several qemu locking sequences ensuring this deadlock no longer occurs. (BZ#697749)

* qemudDomainSaveImageStartVM closed some incoming file descriptor (fd) arguments without informing the caller. The consequent double-closes could cause Domain restoration failure. This update alters the qemudDomainSaveImageStartVM signature to prevent the double-closes. (BZ#681623)

This update also adds the following enhancements:

* The libvirt Xen driver now supports more than one serial port. (BZ#670789)

* Enabling and disabling the High Precision Event Timer (HPET) in Xen domains is now possible. (BZ#703193)

All libvirt users should install this update which addresses this vulnerability, fixes these bugs and adds these enhancements. After installing the updated packages, libvirtd must be restarted ("service libvirtd restart") for this update to take effect.

1.85.4. RHBA-2011:0142: libvirt bug fix update

Updated libvirt packages that fix a bug are now available for Red Hat Enterprise Linux 5.

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.

This update fixes the following bug:

* Previously, when users ran libvirtd on a system with a larger limit for maximum open file descriptors than the default Red Hat Enterprise Linux case of 1024, libvirtd could be aborted with a segmentation fault. This update resolves this issue and the daemon libvirtd behaves as expected. (BZ#667142)

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

1.86. LIBXML2

1.86.1. RHBA-2011:1053: libxml2 bug fix update

Updated libxml2 packages that fixes several bugs are now available for Red Hat Enterprise Linux 5.

The libxml2 library is a development toolbox providing the implementation of various XML standards. One of those standard is XML Schemas, which allow complex validation and checking of document conforming to a schemas describing the allowed structure and content of the document. Another one is XPath, which is a language for addressing parts of an XML document.

This update fixes the following bugs:

* Due to an uninitialized field in one of the private libxml2 XPath data structures, the XPath evaluation could have returned incorrect results. This error has been fixed, the field is now initialized properly, and XPath evaluation returns expected results. (BZ#613860)

* Prior to this update, there were several problems present in the XML Schemas validation component of libxml2. As a result, validating a document against a schema could have been aborted and an error message similar to "xmllint: free(): invalid next size (fast)" could have been displayed under certain circumstances. With this update, the XML Schemas validation component has been fixed so that it works as expected. (BZ#644312)

All users of libxml2 are advised to upgrade to these updated packages, which fix these bugs.

1.87. LINUXWACOM

1.87.1. RHEA-2011:1063: linuxwacom enhancement update

An updated linuxwacom package that adds one enhancement is now available for Red Hat Enterprise Linux 5.

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.

This update adds the following enhancement:

* The linuxwacom package has been updated to support Wacom Cintiq DTU-2231 devices. (BZ#713166)

All users of linuxwacom are advised to upgrade to this updated package, which adds this enhancement.

1.88. LOGROTATE

1.88.1. RHBA-2011:0816: logrotate bug fix update

An updated logrotate package that fixes various bugs is now available for Red Hat Enterprise Linux 5.

The logrotate utility simplifies the administration of multiple log files, allowing the automatic rotation, compression, removal, and mailing of log files.

This update fixes the following bugs:

* When the logrotate.status file was corrupted, the logrotate utility correctly displayed an error message, but did not return a non-zero exit code to indicate a failure. With this update, a patch has been applied to address this issue, and a corrupted logrotate.status file now causes logrotate to terminate with error code 1 as expected. (BZ#461494)

* The "size" configuration option allows a user to specify the minimum size a particular file must reach in order for logrotate to start rotating it. Prior to this update, the maximum supported value of this

option was limited to 4 gigabytes. With this update, this limit has been increased to 16 exabytes. (BZ#484075)

* When used to rotate the /var/log/btmp file, previous versions of the logrotate utility incorrectly changed the permissions of this file to "0644". With this update, a default configuration entry for the /var/log/btmp file has been added to ensure the permissions are correctly set to "0600". (BZ#485553)

* The "missingok" configuration option allows a user to prevent the logrotate utility from reporting an error when a particular log file is missing. Previously, the presence of a wildcard character (typically "*") in a file name caused logrotate to ignore this option. With this update, a patch has been applied to address this issue, and the use of the wildcard characters in the file names no longer causes logrotate to ignore the "missingok" option. (BZ#540119)

* Prior to this update, when the logrotate utility failed to rename a log file, it did not detect this error and incorrectly overwrote or even deleted the original file. To prevent a loss of potentially important logs, this update adapts the utility not to rotate files that cannot be renamed. (BZ#567365)

* Previously, a recursive use of the "include" directive in a configuration file caused the logrotate utility to terminate unexpectedly with a segmentation fault. This update applies an upstream patch that limits the maximum level of recursion, and the recursive use of the "include" directive no longer causes logrotate to crash. (BZ#574784)

* Due to an error in the application logic, the logrotate utility passed an argument with a wildcard to the prerotate and postrotate scripts even when the "sharedscripts" configuration option was specified. With this update, this error no longer occurs, and specifying the "sharedscripts" option now causes logrotate to correctly pass a full path to a particular log. (BZ#579680)

* Previously, the logrotate(8) manual page did not provide a description of the arguments that are passed to the prerotate and postrotate scripts. This update extends the manual page to include this information. (BZ#474013)

* Previously, the "AUTHORS" section of the logrotate(8) manual page did not include the current maintainer of the logrotate utility. This error has been fixed, and logrotate(8) now contains an up-to-date list of authors. Additionally, the manual page now provides a link to the project homepage. (BZ#622059)

* In the logrotate(8) manual page, the description of the "size" configuration option stated that log files are rotated when they grow bigger than the specified file size. Since this description was rather vague, this update corrects the manual page to provide a more accurate description of this option. (BZ#638591)

* Previously, the logrotate(8) manual page did not provide a description of the "-?", "--help", "--verbose", and "--debug" command line options. This error has been fixed, and the manual page now covers all supported command line options as expected. (BZ#642936)

All users of logrotate are advised to upgrade to this updated package, which fixes these bugs.

1.89. LOGWATCH

1.89.1. RHSA-2011:0324: Important logwatch security update

An updated logwatch package that fixes one security issue is now available for Red Hat Enterprise Linux 5 and 6.

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.

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.

A flaw was found in the way Logwatch processed log files. If an attacker were able to create a log file with a malicious file name, it could result in arbitrary code execution with the privileges of the root user when that log file is analyzed by Logwatch. (CVE-2011-1018)

Users of logwatch should upgrade to this updated package, which contains a backported patch to resolve this issue.

1.90. LVM2

1.90.1. RHBA-2011:1071: lvm2 bug fix and enhancement update

An updated lvm2 package that fixes a number of bugs and adds various enhancements is now available for Red Hat Enterprise Linux 5.

IMPORTANT

This update was released as errata RHBA-2011:1071 — lvm2 bug fix and enhancement update.

The lvm2 package contains support for Logical Volume Management (LVM).

Bug Fixes:

BZ#640051

Previously, it was possible to issue a single "lvconvert" command that both allocated and freed the supplied physical extents. This update logically splits this functionality so that an lvconvert command can either allocate or free physical extents, but disallows performing both operations in a single command, with the result that lvcreate is more consistent and easier to use.

BZ#643500

The entire /proc/self/maps file is now read before maps entries are operated upon.

BZ#653643

The command "vgextend --restoremissing" reported success even in the case of partial failure of an operation, which was potentially confusing. Partial failures are now reported as such.

BZ#656394

The default permissions on the /etc/lvm/ directory have been changed to allow non-root users to use required functionality.

BZ#667174

The "lvchange --test" command now exits cleanly.

BZ#671459

An unnecessary and harmless "File-based locking initialization failed." error message that may have occurred during system startup has been removed.

BZ#672816

O_DIRECT is now always used when opening block devices to check for partitioning.

BZ#710618

Reducing a striped logical volume converted to a mirror could have resulted in corruption. This update fixes the rounding operations in striped volume reduction, and a mirror over a striped volume is now reduced successfully.

BZ#709388

The lvmdump command now works properly with the SELinux's Multi-Level Security policy.

BZ#697959

The vgimportclone script triggered a code path in the "lvm" command which accessed already-released memory when a duplicate physical volume (PV) was found. Problematic strings are now saved to a temporary buffer, and this issue no longer occurs.

BZ#651590

If a transient error occurred while a mirror was being repaired, such as a failing device re-appearing, the repair could have failed and a locking error reported. With this update, the mirror repair operation successfully completes in the described situation.

BZ#680961

The lvm2 package has been upgraded to upstream version 2.02.84, which provides a number of bug fixes over the previous version. Those bug fixes also include:

- A possible overflow in maximum stripe size and physical extent has been fixed.
- pvmove polling no longer fails if another process has already cleaned up.
- Error messages issued by the lvcreate command now refer to "free space" rather than "extents".
- A memory leak in the persistent filter creation error path has been plugged.
- The label cache is no longer revalidated immediately after scanning.
- VG (volume group) allocation policy in metadata being invalid could have caused a memory leak, which has been plugged.
- An unrecognized allocation policy in metadata is now ignored rather than aborting the executed command.
- The redundant "No PV label" error message is now suppressed when several PVs are removed without MDAs.
- The vgchange command now only updates VG metadata once when making multiple changes.

- The vgchange command now processes the "-a", "--refresh", "--monitor" and "--poll" options like lvchange does.
- The vgchange command no longer takes a write lock when the "--refresh", "--poll" or "--monitor" options are supplied.
- The lvconvert command now respects the "--yes" and "--force" options when converting an active log.
- If lvm1 metadata is used, partial mode is limited in operation to prevent a crash for operations not yet supported.

Enhancements:

BZ#189462

Invalidated snapshots are now automatically unmounted by dmeventd.

BZ#213942

Tag length restrictions have been removed, and certain punctuation characters, namely / = ! : # and &, are now accepted.

BZ#427298

This update makes it possible to set up a policy of automatic snapshot extension whenever remaining snapshot space drops below a threshhold defined by the new "snapshot_autoextend_threshold" option in the /etc/lvm/lvm.conf configuration file. With this option set, a snapshot either becomes invalidated, as per the previous behavior, or it is extended and automatically continues to function as long as long as free Volume Group space permits.

BZ#433768

The cling allocation policy has been extended to recognize PV (physical volume) tags in the "cling_by_tags" option in lvm.conf.

BZ#644578

A new configurable option, "pv_min_size", has been added to the lvm.conf configuration file. This option can be used to improve performance of commands that scan all devices by setting the pv_min_size value to skip device reading below a certain predefined level.

BZ#659264

The man pages for the pvmove, pvcreate, pvremove, pvresize, pvscan and lvscan commands have been updated and improved.

BZ#644079, BZ#640101

Converting a mirror log type from disk to mirrored is now supported.

BZ#708492

Striped mirrors are now supported.

BZ#680961

The lvm2 package has been upgraded to upstream version 2.02.84, which provides a number of enhancements over the previous version. Those enhancements include:

- Multiple "--addtag" and "--deltag" options can now be supplied as parameters.
- Independent vgchange arguments can now be used together.
- The output from "dmsetup ls --tree" has been added to lvmdump.
- Command processing has been sped up by caching the resolved configuration tree.
- Multiple pvchange command line options can now be specified simultaneously.
- An unnecessary call to unlock during volume deactivation has been eliminated.
- "Fusion-io" is now accepted in the device type filter.
- The "metadata_read_only" option has been added to the global section of the lvm.conf configuration file. If this option is enabled, no operations that change on-disk metadata will be permitted, including automatic repairs of metadata in read-only mode.
- device-mapper devices are now skipped during scans if they contain only error targets or are pseudo-terminal devices.
- The unquoting of quoted double-quotes and backslashes has been sped up.
- CRC32 calculations have been sped up by using a larger lookup table.

Users are advised to upgrade to this updated lvm2 package, which resolves these issues and adds these enhancements.

1.90.2. RHBA-2011:0287: lvm2 bug fix update

An updated lvm2 package that resolves several issues is now available.

The lvm2 package contains support for Logical Volume Management (LVM).

This updated lvm2 package provides fixes for the following bugs:

* With this update, the "File-based locking initialization failed." warning, which was displayed during the system start-up, is now suppressed. (BZ#673975)

* Under certain circumstances, mainly on shared storage systems, the buffered read of a device was used instead of a direct device access. This could result in the use of outdated metadata values. This update ensures that all device scan operations use the direct device access. (BZ#673981)

* This update fixes a faulty initialization which in certain cases lead to a full unconditional rescan of devices. As a result, all lvm operations were slowed down and exhibited poor performance. (BZ#673986)

All users of lvm2 are advised to upgrade to this updated package, which resolves these issues.

1.91. LVM2-CLUSTER

1.91.1. RHBA-2011:0986: lvm2-cluster bug fix and enhancement update

An updated lvm2-cluster package that fixes several bugs and adds various enhancements is now available for Red Hat Enterprise Linux 5.

The lvm2-cluster packages contain support for Logical Volume Management (LVM) in a clustered environment.

This updated lvm2-cluster package ensures that the fixes provided with the Red Hat Enterprise Linux lvm2 advisory are also fixed in a clustered environment. The full list of changes is detailed in the WHATS_NEW file located in the /usr/share/doc/lvm2-[version]/ directory.

This package also provides fixes for the following bugs:

* Wrongly-paired unlocking in the pvchange command has been fixed. (BZ#667517)

* O_DIRECT is now always used when block devices are opened to check for partitioning. (BZ#673615)

* The clvmd daemon now respects the settings in the lvm.conf configuration file when it initializes syslog.

* The exclusive lock now remains unchanged when a device is suspended by the clvmd daemon.

* The clvmd daemon now properly increments the DLM lockspace reference count.

* The clvmd daemon now creates the /var/run/lvm/ directory during initialization if it is missing.

In addition, this updated package provides the following enhancements:

* Activating snapshots of clustered logical volumes is now supported. (BZ#501437)

* The clvmd daemon now supports the "--help" option, and returns proper exit status codes upon exit. (BZ#666991)

* The clvmd daemon now supports the "-f" option, which prevents it from forking, and the description for the "clvmd -d[number]" command has been improved.

Users are advised to upgrade to this updated lvm2-cluster package, which resolves these issues and adds these enhancements.

1.91.2. RHBA-2011:0288: lvm2-cluster bug fix update

An updated lvm2-cluster package that fixes a bug is now available.

The lvm2-cluster package contains support for Logical Volume Management (LVM) in a clustered environment.

This update ensures that bugs fixed by the lvm2 bug fix update advisory are also fixed in a clustered environment, namely the following bug:

* Under certain circumstances, mainly on shared storage systems, the buffered read of a device was used instead of a direct device access. This could result in the use of outdated metadata values. This update ensures that all device scan operations use the direct device access. (BZ#673980)

All users of lvm2-cluster are advised to upgrade to this updated package, which resolves this issue.

1.92. M2CRYPTO

1.92.1. RHBA-2011:1058: m2crypto bug fix update

An updated m2crypto package that fixes various bugs is now available for Red Hat Enterprise Linux 5.

m2crypto allows OpenSSL functions to be called from Python scripts.

This updated m2crypto package includes fixes for the following bugs:

* Prior to this update, the AES_crypt() function did not free a temporary buffer. This caused a memory leak when the function was called repeatedly. This problem has been fixed and the AES_crypt() function now frees memory correctly. (BZ#659881) * Previously, calling the m.2asn1_INTEGER_get() function resulted in an incorrect numerical value for the serial number due to a data type mismatch. As a consequence, the subscription-manager application displayed an error message about the serial number being less than zero. Serial numbers are now handled correctly and no error message appears. (BZ#703648)

All users of m2crypto are advised to upgrade to this updated package, which resolves these bugs.

1.93. MAILMAN

1.93.1. RHSA-2011:0307: Moderate mailman security update

An updated mailman package that fixes multiple security issues is now available for Red Hat Enterprise Linux 4 and 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.

Mailman is a program used to help manage email discussion lists.

Multiple input sanitization flaws were found in the way Mailman displayed usernames of subscribed users on certain pages. If a user who is subscribed to a mailing list were able to trick a victim into visiting one of those pages, they could perform a cross-site scripting (XSS) attack against the victim. (CVE-2011-0707)

Multiple input sanitization flaws were found in the way Mailman displayed mailing list information. A mailing list administrator could use this flaw to conduct a cross-site scripting (XSS) attack against victims viewing a list's "listinfo" page. (CVE-2008-0564, CVE-2010-3089)

Red Hat would like to thank Mark Sapiro for reporting the CVE-2011-0707 and CVE-2010-3089 issues.

Users of mailman should upgrade to this updated package, which contains backported patches to correct these issues.

1.94. MAN

1.94.1. RHEA-2011:0994: man bug fix and enhancement update

An updated man package that fixes one bug and adds one enhancement is now available for Red Hat Enterprise Linux 5.

The man package provides the man, apropos, and whatis tools for finding information and documentation about your Linux system.

This update fixes the following bug:

* Prior to this update, the variable name TMPFILEDIR was not defined in the makewhatis script. Due to this problem, users could lose their entire file system if they defined TMPFILEDIR=/ in the

environment. In case of TMPFILEDIR=/tmp, the tmp folder could be lost. This update defines the variable TMPFILEDIR in the makewhatis and no more loss of files occur. (BZ#560585)

This update also adds the following enhancement:

* Prior to this update, the man package did not support the man-pages-overrides subdirectory. Due to this lack, the man-pages-overrides package did not work correctly. This update adds this subdirectory. Now, man-pages-overrides works as expected.(BZ#558732)

All man users are advised to upgrade to this updated package, which fixes this bug and adds this enhancement.

1.95. MCELOG

1.95.1. RHBA-2011:0512: mcelog bug fix update

An updated mcelog package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The mcelog package contains a daemon that collects and decodes Machine Check Exception (MCE) data on AMD64 and Intel 64 machines.

* On some systems, mcelog was able to read beyond the last page of the SMBIOS tables. This caused a failure in the mmap() call, the "Cannot mmap SMBIOS tables" error message was issued and the user was unable to run mcelog further. Now, the range for the mmap() calls has been lowered and the bug no longer occurs. (BZ#698122)

Users of mcelog are advised to upgrade to this updated package, which fixes this bug.

1.95.2. RHBA-2011:0377: mcelog bug fix update

An updated mcelog package that fixes a bug is now available for Red Hat Enterprise Linux 5.

The mcelog daemon collects and decodes Machine Check Exception (MCE) data on 64-bit x86 machines.

This update fixes the following bug:

* The mcelog daemon shipped with Red Hat Enterprise Linux 5 does not support all processors. Previously, mcelog did not check whether the system is supported or not before adding a cronjob. Consequent to this, an attempt to use it on an unsupported system caused the following email message to be sent to a system administrator every hour:

mcelog: Unknown Intel CPU type family [cpu_family] model [model]

With this update, mcelog has been adapted to ensure that the system is supported before adding a cronjob, so that system administrators no longer receive these messages. (BZ#621669)

Users of mcelog are advised to upgrade to this updated package, which resolves this issue.

1.96. MKINITRD

1.96.1. RHBA-2011:1017: mkinitrd bug fix update

Updated mkinitrd packages that fix two bugs are now available for Red Hat Enterprise Linux 5.

The mkinitrd utility creates file system images for use as initial RAM disk (initrd) images.

This update fixes the following bugs:

* Prior to this update, modules and options contained in the configuration files (*.conf) in the /etc/modprobe.d/ directory were ignored when generating a new initrd image. This update resolves the problem by adding the configuration files to the list of files checked for modules and options during the initrd image creation. (BZ#564392)

* Prior to this update, the cryptomgr module was not installed in the initrd image. As a result, because the Linux kernel versions 2.6.18-258 and later require cryptomgr to be installed in the initrd image when using the dm-crypt subsystem, it was not possible to decrypt any Linux Unified Key Setup (LUKS) partition when dm-crypt was used. This update resolves the problem by adding cryptomgr to the initrd image when dm-crypt is used so that decrypting LUKS partitions now works as expected. (BZ#694534)

All mkinitrd users are advised to upgrade to these updated packages, which fix these bugs.

1.96.2. RHBA-2011:0430: mkinitrd bug fix update

Updated mkinitrd packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The initrd image is an initial RAM disk that is loaded by a boot loader before the Linux kernel is started. The mkinitrd utility creates the initrd file system image.

This update fixes the following bug:

* When creating the initrd file, the mkinitrd utility reads the configuration to determine what kernel modules to load and which module options to use. Previously, the mkinitrd utility only read the /etc/modprobe.conf configuration file. This update corrects this error, and when the /etc/modprobe.conf file does not exist, mkinitrd now attempts to read the configuration from the files located in /etc/modprobe.d/ instead. (BZ#694052)

All users of mkinitrd are advised to upgrade to these updated packages, which fix this bug.

1.97. MOD_AUTHZ_LDAP

1.97.1. RHBA-2011:0482: mod_authz_ldap bug fix update

An updated mod_authz_ldap package that fixes one bug is now available for Red Hat Enterprise Linux 5.

mod_authz_ldap is a module for the Apache HTTP Server. This module provides support for authenticating users against an LDAP database.

This update fixes the following bug:

* Previously, the RPM spec file did not mark /etc/httpd/conf.d/authz_ldap.conf as a configuration file, which allowed any subsequent update to this package to overwrite this file regardless of its local changes. With this update, the spec file has been corrected to mark /etc/httpd/conf.d/authz_ldap.conf as "%config(noreplace)", so that the file is no longer overwritten upon an update. (BZ#533837)

All users of mod_authz_ldap are advised to upgrade to this updated package, which fixes this bug.

1.98. MOD_NSS

1.98.1. RHBA-2011:0411: mod_nss bug fix update

An updated mod_nss package that fixes NSS database permissions when upgrading is now available for Red Hat Enterprise Linux 5.

The mod_nss module provides strong cryptography for the Apache HTTP Server via the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, using the Network Security Services (NSS) security library.

This update addresses the following bug:

* The NSS database initializing sequence changed in mod_nss 1.0.8. As of this version, the database is initialized in each Apache child rather than in the main process. This change adheres to the PKCS #11 specification which does not allow forking after a token is initialized. As a result the NSS database needs to be readable by the user that Apache runs as. When mod_nss 1.0.8 is newly installed, it generates a new database and ensures file ownership is correct (ie is root:apache, mode 0640).

Previously, however, a bug in the %postinstall script meant the necessary read permissions were not added correctly when upgrading from mod_nss 1.0.3 to 1.0.8. As a consequence, after upgrading from mod_nss 1.0.3 to mod_nss 1.0.8, the Apache server failed to start. This update corrects the error in the %postinstall script and upgrading from mod_install 1.0.3 to 1.0.8 now adds the necessary read permissions (and Apache starts as expected after upgrading).

Note: as described above, this bug only presented when upgrading from mod_install 1.0.3 to 1.0.8. New installs of 1.0.8 were not affected by this bug. (BZ#679748)

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

1.99. MYSQL

1.99.1. RHBA-2011:0494: mysql bug fix update

Updated mysql packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

MySQL is a multi-user, multithreaded SQL database server.

These updated mysql packages provide fixes for the following bugs:

* Resolving queries containing a subquery with the DISTINCT and ORDER BY subclauses could have triggered a memory leak causing the query resolution to fail or the server to terminate unexpectedly if it had to process an extensive number of rows. With this update, the respective upstream patch has been applied and the queries are resolved correctly. (BZ#692953)

* Previously, the MySQL client could have corrupted input lines exceeding one megabyte due to errors in the code for handling the line splitting. This update changes the underlying code and the client saves such input lines correctly. (BZ#700497)

All users of mysql are advised to upgrade to these updated packages, which fix these bugs.

1.100. NAUTILUS

1.100.1. RHBA-2011:0440: nautilus bug fix update

Updated nautilus packages that fix two bugs are now available for Red Hat Enterprise Linux 5.

The Nautilus file manager integrates access to files, applications, media, and the Internet, and is a core component of the GNOME desktop project.

This update fixes the following bugs:

* Previously, Nautilus did not check input events correctly. Due to this problem, folders were opened twice if the user double-clicked already selected folders. This update adds additional checks to determine whether the same or another item is clicked. Now, double-clicking these items behaves as expected. (BZ#427580)

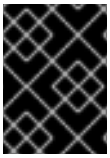
* Previously, Nautilus did not respect the environment umask setting. Due to this problem, newly created files which were internally copied from templates, inherited permissions from the original file. This update adds a flag to respect the umask setting. Now, newly created files, which are internally copied from templates, have the correct permissions according to the desired umask. (BZ#459687)

All nautilus users are advised to upgrade to these updated packages, which fix these bugs.

1.101. NET-SNMP

1.101.1. RHBA-2011:1076: net-snmp bug fix and enhancement update

Updated net-snmp packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 5.



IMPORTANT

This update was released as errata RHBA-2011:1076 — net-snmp bug fix and enhancement update.

The net-snmp packages provide various libraries and tools for the Simple Network Management Protocol (SNMP), including an SNMP library, an extensible agent, 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 management information base (MIB) browser.

Bug Fixes:

BZ#554956

When running on a machine with an aliased network interface, a small memory leak may have occurred and the **snmpd** daemon may have incorrectly spammed syslog with the following message:

```
error on subcontainer '' insert (-1)
```

Although the message itself is completely harmless, it may have filled the system log. This update adapts the underlying source code to make sure the **snmpd** no longer leaks memory or produces the aforementioned message when processing aliased interfaces.

BZ#556824

When running on a big-endian machine, the **snmpd** daemon incorrectly mixed pointers to integers of a different size, and reported wrong indexes of the **UDP-MIB::udpTable** table. With this update, this error no longer occurs, and **snmpd** now reports correct indexes.

BZ#557758

When loading a list of installed RPM packages for the **HOST-RESOURCE::hrSWInstalledTable** table, a rare race condition may have occurred if an RPM package was being updated, installed, or removed at the same time, causing the **snmpd** daemon to terminate unexpectedly with a segmentation fault. With this update, **snmpd** has been adapted to recover from such a situation, and no longer crashes in this scenario.

BZ#561875

When retrieving data for the Remote Network Monitoring Management Information Base (RMON-MIB), the **snmpd** daemon may have leaked file descriptors. As a result, the file descriptors available to the **snmpd** process may have been exhausted, rendering the daemon unable to respond to SNMP requests. With this update, all unnecessary file descriptors are appropriately closed, and **snmpd** now works as expected.

BZ#561882

When a network interface was not active and the **snmpd** service was unable to obtain its real speed from the kernel, it incorrectly reported an erroneous value of the **IF-MIB::ifSpeed** object. This update corrects the **snmpd** daemon to report the correct speed if the kernel provides it, and not to report the speed of a disabled network at all if it cannot be obtained.

BZ#562376, **BZ#653780**

Prior to this update, the **snmpd** daemon did not initialize the structures for the **IP-MIB::ipSystemStatsTable** and **IP-MIB::ipIfStatsTable** tables properly. Consequent to this, when a counter in these tables exceeded 32 bits, the following error message may have been written to the system log:

```
looks like a 64bit wrap, but prev!=new
```

This update corrects the initialization of the aforementioned tables, resolving this issue.

BZ#574035

Prior to this update, when a user provided a passphrase that was too short, various SNMP utilities such as **snmpget** or **snmpwalk** incorrectly returned exit code 0. This error no longer occurs, and the SNMP utilities now return a non-zero exit code in this scenario.

BZ#584769

Previously, the **logrotate** configuration file shipped with the net-snmp packages restarted the **snmpd** daemon whenever the **/var/log/snmpd.log** file was rotated. However, this led to an unnecessary interruption of the SNMP service, and may have negatively affected several SNMP counters. With this update, the aforementioned configuration file has been adapted to only notify the running **snmpd** daemon that the log file should be reopened, and no longer interrupts the SNMP service.

NOTE

By default, the **snmpd** daemon writes messages to the system log (that is, the **/var/log/messages** file). Since logging to the **/var/log/snmpd.log** file is optional and must be enabled manually, most users were not affected by this bug.

BZ#587617

The upstream test suite that was previously shipped as part of the source RPM package did not work with the TCP and UDP protocols for IPv6, and reported false errors. This update adapts the test suite to work with IPv6 as expected.

BZ#587785

When responding to an SNMP **GET** request of an unknown row in the **IF-MIB::ifTable** table, the Net-SNMP daemon incorrectly returned a **noCreation** error. This update applies a patch that resolves this issue, and the **snmpd** daemon now correctly returns a **noSuchInstance** error as specified by the SNMP standards.

BZ#591416

During recompilation of the net-snmp source package, the **configure** script reported an error. Although this error was completely harmless and did not affect the resulting build in any way, it unnecessarily polluted the output of the **rpmbuild** command. To prevent this, the error in the header ordering has been fixed so that the package can be rebuilt with no error messages.

BZ#595322

Prior to this update, index values of the **HOST-RESOURCES-MIB::hrFSTable** and **HOST-RESOURCES-MIB::hrStorageTable** tables were not persistent across device remounts (that is, a particular index may have been different before and after a device was unmounted and mounted again). With this update, the **snmpd** daemon has been updated to keep track of mounted and unmounted devices in order to retain the same indexes across remounts.

BZ#600319

Previously, the **snmpd** daemon was updated to send SNMP responses to broadcast requests from the same interface on which the SNMP was received. However, this update also introduced an error which prevented it from sending responses to unicast request on multihomed machines (that is, on machines with multiple network interfaces, each facing a different network). This update corrects this error so that the **snmpd** daemon is now able to both answer unicast requests on multihomed machines and send responses to broadcast requests from the same interface on which the request was received.

BZ#630905

Due to a possible race condition, the **snmpd** daemon may have failed to count some processes when populating the **UCD-SNMP-MIB::prTable** table. With this update, the underlying source code has been adapted to prevent such a race condition so that all processes are now counted as expected.

BZ#645303

Due to a possible overflow of a 32-bit signed integer, the **snmptranslate** tool may have reported wrong ranges of objects with the Unsigned32 syntax. This update adapts **snmptranslate** to use 64-bit values for integer ranges, so that the utility no longer produces incorrect Unsigned32 ranges.

BZ#645317

Previously, the **snmpd** service returned an incorrect value of the **IP-MIB::ipv6InterfaceForwarding** object: for **forwarding** it reported **0** instead of **1**, and for **notForwarding** it reported **1** instead of **2**. With this update, this error no longer occurs, and **snmpd** now reports the value of **IP-MIB::ipv6InterfaceForwarding** in accordance with RFC 4293.

BZ#654384

Previously, the **snmpd** daemon strictly implemented RFC 2780. However, this specification no longer scales well with modern big storage devices with small allocation units, and consequently, **snmpd** reported a wrong value of the **HOST-RESOURCES-MIB::hrStorageSize** object when working with a large file system (larger than 16TB), because the accurate value would not fit into Integer32 as specified in the RFC. To address this issue, this update adds a new option to the **/etc/snmp/snmpd.conf** configuration file, **realStorageUnits**. By changing the value of this option to **0**, users can now enable recalculating all values in **hrStorageTable** to ensure that the multiplication of **hrStorageSize** and **hrStorageAllocationUnits** always produces an accurate device size. On the other hand, the values of **hrStorageAllocationUnits** are artificial and do not represent the real size of the allocation unit on the storage device.

BZ#659354

When running on a big-endian machine, the **snmpd** daemon reported wrong values of storage sizes in the **HOST-RESOURCES-MIB::hrStorageTable** table. This was caused by incorrect use of pointers to integers of a different size. With this update, the **snmpd** daemon has been adapted to use pointers to integer values in the **HOST-RESOURCES-MIB::hrStorageTable** implementation. As a result, the sizes in the aforementioned table are now reported correctly.

BZ#663863

When an object identifier (OID) was out of the subtree registered by the **proxy** statement in the **/etc/snmp/snmpd.conf** configuration file, the previous version of the **snmpd** daemon failed to use a correct OID of proxied **GETNEXT** requests. With this update, **snmpd** now adjusts the OIDs of proxied **GETNEXT** requests correctly and sends correct requests to the remote agent as expected.

BZ#676669

After processing the **SIGUP** signal, the **snmpd** daemon may have stopped to report a correct value in the **HOST-RESOURCES-MIB::hrStorageTable** table. This update corrects this error so that when the **SIGHUP** signal is processed, the **snmpd** daemon now provides correct values in **HOST-RESOURCES-MIB::hrStorageTable**.

BZ#676955

The previous version of **snmptrapd**, the Net-SNMP daemon for processing traps, leaked memory when processing incoming SNMP traps in embedded Perl. This caused the amount of consumed memory to grow over time, making the memory consumption was even larger if the daemon was processing SNMPv1 traps. With this update, the underlying source code has been adapted to prevent such memory leaks, and processing incoming SNMP traps in embedded Perl no longer increases the memory consumption.

BZ#680347

The previous version of the **snmpd** daemon failed to detect newly added or activated interfaces, and did not show them in the **IPV6-MIB::ipv6IfTable** table. With this update, a patch has been applied to address this issue, and the **snmpd** daemon now properly refreshes the table whenever a new interface appears.

BZ#683142

Prior to this update, the **snmpd** daemon did not detect errors when accessing the **/proc** file system. Consequent to this, an attempt to read information about an exited process while gathering information for a **HOST-RESOURCES-MIB::hrSWRunTable** table caused the daemon to terminate unexpectedly with a segmentation fault. This update adapts the underlying source code to make sure that such errors are now properly detected, and **snmpd** no longer crashes when populating **HOST-RESOURCES-MIB::hrSWRunTable**.

BZ#704443

The previous version of the **snmpd** daemon incorrectly processed requests with malformed Basic Encoding Rules (BER), namely with the wrong **type** field of **Community**, **RequestID**, **Error-status**, and **Error-index** attributes. The updated **snmpd** daemon properly checks encoding of incoming packets and silently drops malformed requests as required by SNMP RFCs.

BZ#556842

Previously, the *SYNOPSIS* section of the **snmpnetstat**(1) manual page incorrectly listed the **-CP** option instead of **-Cp**. This error has been fixed so that the aforementioned manual page no longer contains misleading information.

BZ#583807

In the description of the **linkUpDownNotifications** directive, the **snmpd.conf**(5) manual page treats the **linkUp** and **linkDown** notifications as containing the **ifIndex**, **ifAdminStatus**, and **ifOperStatus** objects. Previously, the **snmpd** daemon did not include these objects in outgoing notifications. With this update, the **snmpd** daemon has been adapted to add these objects to the outgoing notifications as described in the manual page.

BZ#613584

Prior to this update, the help messages of various SNMP-related tools and their corresponding manual pages (such as the **snmptrapd**(8) page) incorrectly suggested **-D** *token* as a valid syntax of the **-D** command line option. This update corrects this error, and both manual pages and help messages of the affected tools now strictly use the **-D***token* syntax as expected.

Enhancements:

BZ#664523

With this update, the **UCD-SNMP-MIB::dskTable** table has been enhanced to report 64-bit statistics of available, used, and free disk space. As a result, the table now provides the following new columns: **dskTotalLow**, **dskTotalHigh**, **dskAvailLow**, **dskAvailHigh**, **dskUsedLow**, and **dskUsedHigh**.

All users of net-snmp are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

1.102. NETWORKMANAGER

1.102.1. RHBA-2011:1023: NetworkManager bug fix update

Updated NetworkManager packages that fix two bugs are now available for Red Hat Enterprise Linux 5.

NetworkManager is a system network service that manages network devices and connections, attempting to keep active network connectivity when available. It manages Ethernet, wireless, mobile broadband (WWAN), and Point-to-Point Protocol over Ethernet (PPPoE) devices, and provides virtual private network (VPN) integration with a variety of different VPN services.

This update fixes the following bugs:

* Prior to this update, stopping the messagebus service, either manually or during a routine system shutdown, could cause certain NetworkManager components to terminate unexpectedly with a segmentation fault. With this update, the underlying source code is modified to target this issue. Now, NetworkManager components exit with a 0 return code when the messagebus service is stopped. (BZ#580393)

* Prior to this update, connecting to WPA Enterprise networks with CHAP authentication could cause the network dialog to terminate unexpectedly with a segmentation fault due to an incorrect index. This update modifies the source code to use the correct index. Now, the network dialog works as expected. (BZ#644256)

All NetworkManager users are advised to upgrade to these updated packages, which fix these bugs.

1.103. NFS-UTILS

1.103.1. RHBA-2011:1048: nfs-utils bug fix and enhancement update

An updated nfs-utils package that fixes various bugs and adds one enhancement is now available for Red Hat Enterprise Linux 5.

The nfs-utils package provides a daemon for the kernel Network File System (NFS) server, and related tools such as the mount.nfs, umount.nfs, and showmount programs.

This update fixes the following bugs:

* With an automounter in use, mounting a large number of NFS file systems (that is, 500 and more) over the TCP protocol at the same time caused the process to run out of privileged ports. Consequent to this, many of these mount attempts may have failed with an error message written to the system log. This update applies a patch to wait for a period of time specified by the "retry=" option before attempting to establish a connection with the NFS mount daemon again. (BZ#240790)

* Due to an error in the RPM spec file, the rpc.statd daemon may have been incorrectly running as the root user. This error has been fixed so that rpc.statd now runs as rpcuser. (BZ#495066)

* By providing the "-d" command line option, the rpc.gssd daemon allows a user to specify a directory or directories in which to look for Kerberos credential files. Previously, an attempt to specify a value other than "/tmp" caused the daemon to fail with the following error:

rpc.gssd: ccachedir path name too long

With this update, this error no longer occurs, and the "-d" option can now be used as expected. (BZ#498134)

* Due to an error in the RPM spec file, the nfsnobody user was assigned a different UID and GID on 32-bit and 64-bit architectures. This error has been fixed, and the nfsnobody user is now created with UID and GID 65534 on both 32-bit and 64-bit architectures. (BZ#511876)

* When an NFS file system was mounted over the UDP protocol from a server that did not allow the use of the TCP protocol, an attempt to unmount it failed, because the umount.nfs utility incorrectly used

TCP. With this update, a patch has been applied to address this issue so that umount.nfs no longer uses an incorrect protocol. (BZ#513466)

* Previously, the nfs and nfslock init scripts incorrectly returned exit code 0 even when the respective service was stopped. This update corrects this error, and when the corresponding service is stopped, these init scripts now return a non-zero exit code as expected. (BZ#534133, BZ#542020)

* The NFS mount daemon allows a user to disable a particular version of the NFS protocol by changing the value of the "MOUNTD_NFS_V1" option in the /etc/sysconfig/nfs configuration file to "no". Previously, an attempt to unmount a shared file system from a server with such configuration failed with an error. This update applies a patch that addresses this issue so that shared file systems can now be unmounted as expected. (BZ#595675)

* Prior to this update, running "nfsstat -s -o rpc" command produced output with incorrect labels in a table header. With this update, the underlying source code has been adapted to make sure that all columns now have the correct name. (BZ#617669)

As well, this update adds the following enhancement:

* The mount.nfs4 utility has been updated to provide a new mount option, "lookupcache=", which allows the NFS client to control how it caches files and directories. (BZ#511312)

All users of nfs-utils are advised to upgrade to this updated package, which fixes these bugs and adds this enhancement.

1.104. NSS

1.104.1. RHSA-2011:0472: Important nss security update

Updated nss packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having important security impact.

Network Security Services (NSS) is a set of libraries designed to support the development of security-enabled client and server applications.

This erratum blacklists a small number of HTTPS certificates by adding them, flagged as untrusted, to the NSS Builtin Object Token (the libnssckbi.so library) certificate store. (BZ#689430)

Note: This fix only applies to applications using the NSS Builtin Object Token. It does not blacklist the certificates for applications that use the NSS library, but do not use the NSS Builtin Object Token (such as curl).

All NSS users should upgrade to these updated packages, which correct this issue. After installing the update, applications using NSS must be restarted for the changes to take effect.

1.105. NSS_LDAP

1.105.1. RHBA-2011:1030: nss_ldap bug fix update

An updated nss_ldap package that fixes various bugs is now available for Red Hat Enterprise Linux 5.

The nss_ldap package contains the nss_ldap and pam_ldap modules. The nss_ldap module allows applications to retrieve information about users and groups from a directory server. The pam_ldap

module allows a directory server to be used by PAM-aware applications to verify user passwords.

This update fixes the following bugs:

* Prior to this update, using the getent utility to retrieve information about a group with a large number of users could take a very long time. This update applies a backported patch that addresses this issue and significantly improves the performance. (BZ#646329)

* When the "netgroup" entry in the /etc/nsswitch.conf configuration file is set to "ldap files" and the connection to an LDAP server cannot be established, the system is supposed to search local files for netgroups instead. Previously, querying such a system for netgroups could incorrectly produce an empty list. This update corrects this error, and when the "netgroup" entry is set to "ldap files" and the LDAP server is unavailable, local files are now searched as expected. (BZ#664609)

* When a system is configured to use LDAP accounts and a password expires, the relevant user is prompted to change it upon the next login. Previously, the pam_ldap module incorrectly allowed users to re-use their old passwords. With this update, this error no longer occurs, and users are no longer allowed to enter the same password when prompted to change it. (BZ#667758)

* Due to a possible assertion failure in the nss_ldap module, the previous version of the nss_ldap package may have caused various applications that rely on the libldap library to terminate unexpectedly. With this update, a patch has been applied to prevent this assertion failure, resolving this issue. (BZ#688601)

All users of nss_ldap are advised to upgrade to this updated package, which fixes these bugs.

1.105.2. RHBA-2011:0514: nss_ldap bug fix update

An updated nss_ldap package that fixes a bug is now available for Red Hat Enterprise Linux 5.

[Updated 20 May 2011] This advisory has been updated with the correct product name (that is, Red Hat Enterprise Linux 5) in the Details section. The package included in this revised update has not been changed in any way from the package included in the original advisory.

The nss_ldap package contains nss_ldap, a module which allows applications to retrieve information about users, groups, netgroups, from directory servers, and pam_ldap, which allows PAM-aware applications to check users passwords with the aid of a directory server.

This updated nss_ldap package fixes the following bug:

* Previously, if the server closed the connection, the client did not receive any results and failed with the following error, which was caused by the client attempting to parse results which it had not received:

ldap_result: Assertion `ld != ((void *)0)' failed.

With this update, the nss_ldap checks if the server is available while running and finishes with an appropriate error code if the connection fails. (BZ#703831)

All users of nss_ldap are advised to upgrade to this updated package, which resolves this bug.

1.106. NTP

1.106.1. RHBA-2011:0980: ntp bug fix and enhancement update

An updated ntp package that fixes various bugs and provides an enhancement is now available for Red Hat Enterprise Linux 5.

The Network Time Protocol (NTP) is used to synchronize a computer's time with a referenced time source.

This updated ntp package includes fixes for the following bugs:

* The ntpd man pages suggested that the "-L" command option could be issued without an argument. However, the user needs to define the virtual interfaces as arguments of the option. This update corrects the ntp help page. (BZ#460434)

* Prior to this update, if the /usr directory was mounted on an NFS file system, the ntpd service could not be started before the netfs service. This update moves the NTP applications to the /sbin directory so the user may change the ntpd startup priority to start prior to the netfs service. Note that if you wish to mount NFS version 4 with Kerberos authentication, you should consider changing the ntpd startup priority to start prior to the netfs service. Otherwise authentication may fail due to the non-synchronized date. (BZ#470945)

* Prior to this update, verifying the ntp package with the "rpm -V" command failed on the package configuration file if the configuration file had changed. However, changes to the configuration file should not impact the verification test. This update adapts the spec file and the package verify test passes successfully. (BZ#481151)

* The ntpd daemon could terminate unexpectedly due to a low memory lock limit. With this update, the memory lock limit has been doubled. (BZ#575874)

* The "-q" command line option causes the ntpd service to exit immediately after the clock is set. Prior to this update, the man page ntpd(8) did not document that this only occurs if there are servers configured for ntpd to set the clock against. The user could conclude that ntpd was misbehaving when it did not quit if run with the "-q" switch but with no configured servers. With this update, the ntpd(8) man page notes that "ntpd -q" only exits if used to set the clock with configured servers. (BZ#591838)

* Prior to this update, the ntpd daemon could terminate unexpectedly with a segmentation fault on a machine with more than 512 local IP addresses. This happened because of a limit set for scanning. With this update, the limit scan has been changed to scan to the maximum number of interfaces and the ntpd daemon no longer crashes in such circumstances. (BZ#661934)

* Prior to this update, the ntp-keygen(8) patch man page contained multiple typos. This update fixes the typos. (BZ#664524, BZ#664525)

* The "ntpstat" command printed an incorrect maximum error estimate. This occurred because the "time correct to within" value did not include the root delay. With this update, the value includes the root delay and the displayed "time correct to within" value is correct. (BZ#679034)

In addition, this updated ntp package provides the following enhancement:

* Prior to this update, the ntpd daemon did not allow the specification of multiple interfaces which it should be listening on. With this update, the user can define multiple interfaces the daemon should be listening on. (BZ#528799)

All ntp users are advised to upgrade to this updated package, which resolves these issues and provides this enhancement.

1.107. NUMACTL

1.107.1. RHBA-2011:0825: numactl bug fix update

An updated numactl package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The numactl package adds a 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 update fixes the following bug:

* Under certain circumstances, having an environment of three numa nodes resulted in a memory corruption, which had a negative impact on performance. This problem has been fixed in this update so that the memory corruption does not occur anymore. (BZ#705309)

All users requiring numactl should upgrade to this updated package, which fixes this bug.

1.108. OPENAIS

1.108.1. RHBA-2011:1012: openais bug fix update

An updated openais package that fixes various bugs is now available for Red Hat Enterprise Linux 5.

The Application Interface Specification (AIS) is an API and a set of policies for developing applications that maintain services 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 executable, OpenAIS service handlers, default configuration files, and an init script.

This update fixes the following bugs:

* When there were a lot of nodes left at the same time during the controlled shutdown of the Corosync Cluster Engine, the nodes had to wait for the token timeout for each node. As a result, this unintended behavior slowed down the whole shut down process. The problem has been fixed so that a JOIN message is now sent out with the node removed. (BZ#645299)

* Previously, the amount of open files limit was not handled gracefully. The problem has been fixed in this update so that if the open files limit is now reached, the published server listening socket is withdrawn. Then when a connection is closed, the server listening socket is republished, if necessary. (BZ#611434)

* When the SysV semaphores or Shared Memory (SHM) limit was exceeded, a client could have looped forever. This bug has been fixed and the "SA_AIS_ERR_NO_SPACE" error value is returned if one of the limits is exceeded. (BZ#561546)

* Previously, if the token was lost, the old ring ID information was restored, causing a commit token to be accepted when it should have been rejected. This erroneously accepted commit token led to an assertion, which has been fixed in this update. (BZ#623176)

* When the ring ID file for the processor was less then 8 bytes, totemsrp asserted as a result. This has been fixed so that OpenAIS will now create a fresh ring ID file data when the incorrect number of bytes is read from the ring ID file. (BZ#675206)

All users of openais are advised to upgrade to this updated package, which fixes these bugs.

1.108.2. RHBA-2011:0495: openais bug fix update

An updated openais package that fixes various bugs is now available for Red Hat Enterprise Linux 5.

The Application Interface Specification (AIS) is an API and a set of policies for developing applications that maintain services 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 executable, OpenAIS service handlers, default configuration files and an init script.

This update fixes for the following bugs:

* When a system limit for semaphores or shared memory was exceeded on SysV, the openais client sometimes went into a loop. With this update, the openais client handles the situation properly, and no longer enters an infinite loop when either of these limits is exceeded. (BZ#694180)

* When the OpenAIS limit for open files was exceeded, the openais executable terminated unexpectedly. With this update, if the limit is reached, the published server listening socket is withdrawn and the connection closes without causing any crashes. (BZ#694181)

* Previously, if a token was lost in the recovery state, the openais executable sometimes accepted a commit token with old ring ID information. This resulted in an unexpected termination. This bug has been fixed and lost tokens are now handled properly. (BZ#694182).

* When the ring ID file for a processor was less then 8 bytes long, totemsrp terminated unexpectedly. Now, OpenAIS always creates fresh ring ID file data when an incorrect number of bytes are read from the ring ID. (BZ#694183)

All users of openais are advised to upgrade to this updated package, which fixes these bugs.

1.109. OPENIB

1.109.1. RHBA-2011:1056: openib bug fix update

An updated openib package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The openib package provides the user space initialization scripts for the kernel InfiniBand drivers.

* Prior to this update, bash encountered a syntax error in the ifup-ib script on systems with an active InfiniBand network interface but without an explicitly set maximum transmission unit (MTU). Due to this error, a boot process error message was displayed during InfiniBand's interface initialization that too many arguments were used. This update modifies the ifup-ib initialization script so that it runs without errors. (BZ596823)

All InfiniBand users are advised to upgrade to this updated openib package, which fixes this bug.

1.110. OPENLDAP

1.110.1. RHSA-2011:0346: Moderate openldap security and bug fix update

Updated openldap packages that fix one security issue and one bug 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 authentication failures being passed from an OpenLDAP slave to the master. If OpenLDAP was configured with a chain overlay and it forwarded authentication failures, OpenLDAP would bind to the directory as an anonymous user and return success, rather than return failure on the authenticated bind. This could allow a user on a system that uses LDAP for authentication to log into a directory-based account without knowing the password. (CVE-2011-1024)

This update also fixes the following bug:

* Previously, multiple concurrent connections to an OpenLDAP server could cause the slapd service to terminate unexpectedly with an assertion error. This update adds mutexes to protect multiple threads from accessing a structure with a connection, and the slapd service no longer crashes. (BZ#677611)

Users of OpenLDAP should upgrade to these updated packages, which contain backported patches to resolve these issues. After installing this update, the OpenLDAP daemons will be restarted automatically.

1.110.2. RHBA-2011:0178: openldap bug fix update

Updated openldap packages that fix two bugs are now available for Red Hat Enterprise Linux 5.

OpenLDAP is an open source suite of LDAP (Lightweight Directory Access Protocol) applications and development tools. The openldap packages contain configuration files, libraries, and documentation for OpenLDAP.

This update fixes the following bugs:

* When running the slapd service with the ppolicy overlay enabled, an attempt to delete the "userPassword" attribute could cause the service to terminate unexpectedly, leaving the database in a corrupted state. With this update, an upstream patch has been applied to address this issue, and deleting the "userPassword" attribute no longer causes the slapd service to crash. (BZ#669043)

* Prior to this update, the libldap library did not provide the ldap_init_fd() function, even though certain utilities such as cURL rely on it and could not work properly as a result. This update applies a backported upstream patch that implements this API function, so that these tools can now work as expected. (BZ#671341)

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

1.111. OPENMOTIF

1.111.1. RHBA-2011:0964: openmotif bug fix update

An updated openmotif package that fixes a bug is now available for Red Hat Enterprise Linux 5.

The openmotif package includes the Motif shared libraries needed to run applications that are dynamically linked against Motif, as well as the Motif Window Manager (MWM).

This update fixes the following bug:

* Previously, a check that would limit removing a callback to valid windows while the focus is reset was missing in the code. Consequently, destroying a torn-off menu with a submenu mapped caused the application to terminate unexpectedly. With this update, the underlying source code has been modified

to ensure that the focus is reset for valid windows only and destroying a torn-off menu with a submenu mapped now works as expected. (BZ#712073)

All users of openmotif are advised to upgrade to this updated package, which fixes this bug.

1.112. OPENOFFICE.ORG

1.112.1. RHSA-2011:0182: Important openoffice.org security update

Updated openoffice.org packages that fix multiple 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.

OpenOffice.org is an office productivity suite that includes desktop applications, such as a word processor, spreadsheet application, presentation manager, formula editor, and a drawing program.

An array index error and an integer signedness error were found in the way OpenOffice.org parsed certain Rich Text Format (RTF) files. An attacker could use these flaws to create a specially-crafted RTF file that, when opened, would cause OpenOffice.org to crash or, possibly, execute arbitrary code with the privileges of the user running OpenOffice.org. (CVE-2010-3451, CVE-2010-3452)

A heap-based buffer overflow flaw and an array index error were found in the way OpenOffice.org parsed certain Microsoft Office Word documents. An attacker could use these flaws to create a specially-crafted Microsoft Office Word document that, when opened, would cause OpenOffice.org to crash or, possibly, execute arbitrary code with the privileges of the user running OpenOffice.org. (CVE-2010-3453, CVE-2010-3454)

A heap-based buffer overflow flaw was found in the way OpenOffice.org parsed certain Microsoft Office PowerPoint files. An attacker could use this flaw to create a specially-crafted Microsoft Office PowerPoint file that, when opened, would cause OpenOffice.org to crash or, possibly, execute arbitrary code with the privileges of the user running OpenOffice.org. (CVE-2010-4253)

A heap-based buffer overflow flaw was found in the way OpenOffice.org parsed certain TARGA (Truevision TGA) files. An attacker could use this flaw to create a specially-crafted TARGA file. If a document containing this specially-crafted TARGA file was opened, or if a user tried to insert the file into an existing document, it would cause OpenOffice.org to crash or, possibly, execute arbitrary code with the privileges of the user running OpenOffice.org. (CVE-2010-4643)

A directory traversal flaw was found in the way OpenOffice.org handled the installation of XSLT filter descriptions packaged in Java Archive (JAR) files, as well as the installation of OpenOffice.org Extension (.oxt) files. An attacker could use these flaws to create a specially-crafted XSLT filter description or extension file that, when opened, would cause the OpenOffice.org Extension Manager to modify files accessible to the user installing the JAR or extension file. (CVE-2010-3450)

A flaw was found in the script that launches OpenOffice.org. In some situations, a "." character could be included in the LD_LIBRARY_PATH variable, allowing a local attacker to execute arbitrary code with the privileges of the user running OpenOffice.org, if that user ran OpenOffice.org from within an attacker-controlled directory. (CVE-2010-3689)

Red Hat would like to thank OpenOffice.org for reporting the CVE-2010-3451, CVE-2010-3452, CVE-2010-3453, CVE-2010-3454, and CVE-2010-4643 issues; and Dmitri Gribenko for reporting the CVE-2010-3689 issue. Upstream acknowledges Dan Rosenberg of Virtual Security Research as the original reporter of the CVE-2010-3451, CVE-2010-3452, CVE-2010-3453, and CVE-2010-3454 issues.

All OpenOffice.org users are advised to upgrade to these updated packages, which contain backported patches to correct these issues. All running instances of OpenOffice.org applications must be restarted for this update to take effect.

1.113. OPENSM

1.113.1. RHBA-2011:0969: opensm bug fix update

Updated opensm packages that fix one bug are now available for Red Hat Enterprise Linux 5.

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. OpenSM 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.

* Prior to this update, an attempt to connect to a target machine using the SCSI RDMA Protocol (SRP) could cause Small Computer System Interface (SCSI) requests to fail with a timeout. Due to this fault, the mapping of SCSI over InfiniBand was rendered unusable. As a workaround, users are advised not to set the dgid pointer for intra-subnet PR queries. Now, the mapping of SCSI over InfiniBand works as expected. (BZ#645547)

All InfiniBand users are advised to upgrade to these updated packages, which fix this bug.

1.113.2. RHBA-2011:0410: opensm bug fix update

Updated opensm packages that fix a bug are now available for Red Hat Enterprise Linux 5 Extended Update Support.

OpenSM is the OpenIB project's Subnet Manager for InfiniBand networks. These packages provide the opensm daemon, as well as various tools for diagnosing and testing InfiniBand networks.

This update fixes the following bug:

* Previously, an attempt to connect to a target machine using the SCSI RDMA Protocol (SRP) could cause SCSI requests to fail with a timeout. When this happened, this error rendered mapping of SCSI over InfiniBand unusable. This update applies an upstream patch that resolves this issue, and the mapping of SCSI over InfiniBand now works as expected. (BZ#650925)

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

1.114. OPENSSH

1.114.1. RHEA-2011:0420: openssh enhancement update

Updated openssh packages that add one enhancement are now available for Red Hat Enterprise Linux 5.

OpenSSH is OpenBSD's SSH (Secure Shell) protocol implementation. These packages include the core files necessary for both the OpenSSH client and server.

This update adds the following enhancement:

* By default, OpenSSH uses /dev/urandom to reseed the OpenSSL random number generator. Prior to this update, this random number generator was reseeded only once when the sshd service, the ssh

client, or an SSH-aware utility was started. To guarantee sufficient entropy, this update modifies the underlying source code to reseed the OpenSSL random number generator periodically. Additionally, the "SSH_ENTROPY_SOURCE" environment variable has been added to allow users to specify /dev/random as the random number generator. (BZ#690145)

All users of openssh are advised to upgrade to these updated packages, which add this enhancement.

1.115. OPENSSL

1.115.1. RHBA-2011:1010: openssl bug fix and enhancement update

Updated openssl packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

OpenSSL is a toolkit that implements the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, as well as a full-strength general-purpose cryptography library.

This update fixes the following bugs:

* Prior to this update, the "s_server" command refused to handle connections from clients with an unresolvable IP address and terminated with this error message: "getnameinfo failed". This problem has been fixed: the "s_server" command now does not terminate even if the IP address of the client is not resolvable. (BZ#561260)

* Prior to this update, the openssl packages were not fully compliant with the TLS protocol. As a consequence, the system did not accept a connection from a client indicating that it supports the TLS protocol version 4.1. With this update, the server now accepts connections from such clients, which fixes the problem. (BZ#599112)

* Prior to this update, repeatedly loading and unloading the CHIL engine by a calling program caused the calling program to terminate unexpectedly due to a function pointer not being cleared after the engine was unloaded. This bug has been fixed, and the calling program does not crash anymore. (BZ#622003)

* Prior to this update, a check for a weak public key was missing while the Diffie-Hellman key was computed. With this update, the DH_check_pub_key() function call has been added to the DH_compute_key() function, which solves this low impact problem. (BZ#698175)

* The CHIL Engine is used to access Thales or nCipher hardware devices. Prior to this update, when attempting to load the CHIL engine into the openssl utility, the CHIL engine required thread locking callbacks to be set regardless of whether the calling program was multithreaded. With this update, this unexpected requirement has been removed. (BZ#671484)

* Prior to this update, when running a multithreaded OpenSSL client application that tried to connect to a server simultaneously with multiple threads, a TLS protocol error could have occurred. This bug has been fixed in this update and no longer occurs. (BZ#688901)

In addition, this update provides the following enhancements:

* Prior to this update, manual and help pages for various sub-commands of the openssl utility did not specify all the digest algorithms. With this update, the aforementioned pages have been modified, and users are now pointed to the "openssl dgst -h" command that lists all the available digests. (BZ#608639)

* The StartCom Free SSL Certification Authority and VeriSign Class 3 Public Primary Certification Authority - G5 certificates were added to the /etc/pki/tls/certs/ca-bundle.crt file that contains the certificates of trusted certification authorities. (BZ#675671, BZ#617856)

* The support for peer certificates that use the SHA-256 and SHA-512 hashing algorithms is now enabled by default even if the application calls only the SSL_library_init() function without the OpenSSL_add_all_algorithms() call. (BZ#676384)

All users of OpenSSL should upgrade to these updated packages, which fix these bugs and add these enhancements.

1.116. OPENSWAN

1.116.1. RHBA-2011:0388: openswan bug fix update

Updated openswan packages that fix a bug are now available for Red Hat Enterprise Linux 5 Extended Update Support.

Openswan is a free implementation of Internet Protocol Security (IPsec) and Internet Key Exchange (IKE). IPsec uses strong cryptography to provide both authentication and encryption services. These services allow you to build secure tunnels through untrusted networks.

This update fixes the following bug:

* Due to an error in a buffer initialization, the following message may have been written to the /var/log/secure log file during the IKE negotiation:

size ([size]) differs from size specified in ISAKMP HDR ([size])

Consequently, the establishment of secure connections could be significantly delayed. This update applies an upstream patch that resolves this issue, and the establishment of IPsec connections is no longer delayed. (BZ#680044)

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

1.117. PAM_KRB5

1.117.1. RHBA-2011:1016: pam_krb5 bug fix update

An updated pam_krb5 package that fixes various bugs is now available for Red Hat Enterprise Linux 5.

The pam_krb5 package allows applications which use the Pluggable Authentication Modules (PAM) framework to perform password-based authentication using Kerberos 5.

This updated pam_krb5 package includes fixes for the following bugs:

* Previously, multiple authentication attempts may have led to a memory leak when the pam_krb5 module was unloaded. This was caused when the calling application cleaned up the context it used when interacting with the libpam. This has been fixed by preventing the module from being unloaded. (BZ#643962)

* An attempt to set a new Kerberos password using the "passwd" command failed due to a bug which was triggered when the smart card authentication method was enabled and the card was plugged in. This problem has been fixed and users are now able to change the Kerberos password. (BZ#713967)

All users of pam_krb5 are advised to upgrade to this updated package, which resolves these issues.

1.118. PANGO

1.118.1. RHSA-2011:0180: Moderate pango security update

Updated pango and evolution28-pango packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

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.

Pango is a library used for the layout and rendering of internationalized text.

An input sanitization flaw, leading to a heap-based buffer overflow, was found in the way Pango displayed font files when using the FreeType font engine back end. If a user loaded a malformed font file with an application that uses Pango, it could cause the application to crash or, possibly, execute arbitrary code with the privileges of the user running the application. (CVE-2011-0020)

Users of pango and evolution28-pango are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing the updated packages, you must restart your system or restart your X session for the update to take effect.

1.119. PAPS

1.119.1. RHBA-2011:0417: paps bug fix update

An updated paps package that fixes two bugs is now available for Red Hat Enterprise Linux 5.

The paps utility is a command line tool that converts plain text files to PostScript using the Pango library.

This update fixes the following bugs:

* Under certain circumstances, the paps utility could incorrectly typeset output using a heavy weight font. With this update, a patch has been applied to address this issue, and the output is now always rendered with a correct font weight. (BZ#504725)

* Due to an error in the scaling algorithm, running the paps utility with the "--cpi" command line option to specify the characters per inch (CPI) value did not guarantee the output to be scaled correctly. This update corrects the algorithm to work with exact values, and the output is now scaled as expected. (BZ#537450)

Users of paps are advised to upgrade to this updated package, which resolves these issues.

1.120. PARTED

1.120.1. RHBA-2011:1018: parted bug fix update

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

The GNU Parted program allows the creation, destruction, resizing, moving, and copying of 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 problem:

* Running partprobe after creating a new disk label resulted in a traceback. This was caused when a device's sector size was greater than PED_SECTOR_SIZE_DEFAULT (defined as 512 in include/parted/unit.h). A buffer overrun in linux_read() then occurred because the length is greater than the allocated 512 bytes for diobuf. This caused a heap corruption. This patch fixes the issue. (BZ#564104)

All parted users should install the updated package, which resolves this issue.

1.121. PCRE

1.121.1. RHBA-2011:0344: pcre bug fix update

Updated pcre packages that resolve an issue are now available for Red Hat Enterprise Linux 5.

PCRE is a Perl-compatible regular expression library.

These updated pcre packages fix the following bug:

* The pcre package update for Red Hat Enterprise Linux 5.6, the RHEA-2011:0022 enhancement advisory linked to in the References section of this advisory, enabled Unicode properties to support \p{..}, \P{..}, and \X escape sequences. However, compiling certain regular expressions which contained extended classes under a non-UTF-8 PCRE mode failed due to the compilation entering an infinite loop. This has been fixed in this update so that compiling such regular expressions completes as expected. (BZ#669413)

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

1.122. PERL

1.122.1. RHBA-2011:0863: perl bug fix update

Updated perl packages that fix two bugs are now available for Red Hat Enterprise Linux 5.

Perl is a high-level programming language commonly used for system administration utilities and web programming.

This update fixes the following bug:

* Prior to this update, running the CGI::popup_menu method with a default menu choice (that is, the "-default" parameter) that contained a plus sign failed to produce correct HTML output. This update applies a patch that corrects the underlying option parser, and the presence of the plus sign in the name of the default menu choice no longer prevents CGI::popup_menu from producing correct output. (BZ#701631)

* Due to an error in the "threads" module, memory was leaked each time a thread was detached. Over time, this may have caused long-running threaded Perl programs to consume a significant amount of memory. With this update, a patch has been applied to ensure the allocated memory is properly freed

when a thread is detached, and using threads in Perl applications no longer leads to memory leaks. (BZ#701632)

Users of CGI and threads in Perl programs are advised to upgrade to these updated packages, which resolve these issues.

1.123. PHP53

1.123.1. RHSA-2011:0196: Moderate php53 security update

Updated php53 packages that fix three security issues 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.

PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server.

A flaw was found in the way PHP converted certain floating point values from string representation to a number. If a PHP script evaluated an attacker's input in a numeric context, the PHP interpreter could cause high CPU usage until the script execution time limit is reached. This issue only affected i386 systems. (CVE-2010-4645)

A stack memory exhaustion flaw was found in the way the PHP filter_var() function validated email addresses. An attacker could use this flaw to crash the PHP interpreter by providing excessively long input to be validated as an email address. (CVE-2010-3710)

A memory disclosure flaw was found in the PHP multi-byte string extension. If the mb_strcut() function was called with a length argument exceeding the input string size, the function could disclose a portion of the PHP interpreter's memory. (CVE-2010-4156)

All php53 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.

1.124. PIRANHA

1.124.1. RHBA-2011:1059: piranha bug fix update

An updated piranha package that fixes two bugs is now available for Red Hat Enterprise Linux 5.

Piranha provides high-availability and load balancing services for Red Hat Enterprise Linux. Piranha includes various tools to administer and configure the Linux Virtual Server (LVS), as well as the heartbeat and failover components.

This update fixes the following bugs:

* Prior to this update, the pulse daemon aborted unexpectedly with a segmentation fault when trying to reload if there were services without defined servers. This update restarts only running services. Now, the pulse daemon reloads as expected. (BZ#674859)

* Prior to this update, the nanny service forcibly terminated monitoring of all the remaining services as well. This update allows to disable this behavior. A new option in lvs.cf, hard_shutdown, controls this

behavior. Old behavior is retained with the default setting of 1 and manual intervention is required with 0. The remaining monitors are not affected. (BZ#505172)

All Piranha users are advised to upgrade to this updated package, which fixes these bugs.

1.125. POPPLER

1.125.1. RHBA-2011:0517: poppler bug fix update

Updated poppler packages that fix three bugs are now available for Red Hat Enterprise Linux 5.

Poppler is a Portable Document Format (PDF) rendering library, used by applications such as Evince.

This update fixes the following bugs:

* Due to an error in memory allocation, previous versions of poppler may have terminated unexpectedly while rendering certain PDF documents. With this update, the underlying source code has been modified to address this issue, and poppler no longer fails to render such PDF documents. (BZ#698595)

* When working with a PDF document with text spanning multiple columns, text selection may not have followed the flow of the text. This update improves the text selection to respect the text flow. (BZ#703175)

* Prior to this update, certain PDF documents may have been rendered with some characters displayed backwards. With this update, an upstream patch has been applied to ensure that poppler takes into account the horizontal scaling when updating the font, and such PDF documents are now rendered correctly. (BZ#703176)

All users who require poppler are advised to upgrade to these updated packages, which fix these bugs.

1.126. POSTFIX

1.126.1. RHSA-2011:0843: Moderate postfix security update

Updated postfix packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

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.

Postfix is a Mail Transport Agent (MTA), supporting LDAP, SMTP AUTH (SASL), and TLS.

A heap-based buffer over-read flaw was found in the way Postfix performed SASL handlers management for SMTP sessions, when Cyrus SASL authentication was enabled. A remote attacker could use this flaw to cause the Postfix smtpd server to crash via a specially-crafted SASL authentication request. The smtpd process was automatically restarted by the postfix master process after the time configured with service_throttle_time elapsed. (CVE-2011-1720)

Note: Cyrus SASL authentication for Postfix is not enabled by default.

Red Hat would like to thank the CERT/CC for reporting this issue. Upstream acknowledges Thomas Jarosch of Intra2net AG as the original reporter.

Users of Postfix are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing this update, the postfix service will be restarted automatically.

1.126.2. RHSA-2011:0422: Moderate postfix security update

Updated postfix packages that fix two security issues are now available for Red Hat Enterprise Linux 4 and 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.

Postfix is a Mail Transport Agent (MTA), supporting LDAP, SMTP AUTH (SASL), and TLS.

It was discovered that Postfix did not flush the received SMTP commands buffer after switching to TLS encryption for an SMTP session. A man-in-the-middle attacker could use this flaw to inject SMTP commands into a victim's session during the plain text phase. This would lead to those commands being processed by Postfix after TLS encryption is enabled, possibly allowing the attacker to steal the victim's mail or authentication credentials. (CVE-2011-0411)

It was discovered that Postfix did not properly check the permissions of users' mailbox files. A local attacker able to create files in the mail spool directory could use this flaw to create mailbox files for other local users, and be able to read mail delivered to those users. (CVE-2008-2937)

Red Hat would like to thank the CERT/CC for reporting CVE-2011-0411, and Sebastian Krahmer of the SuSE Security Team for reporting CVE-2008-2937. The CERT/CC acknowledges Wietse Venema as the original reporter of CVE-2011-0411.

Users of Postfix are advised to upgrade to these updated packages, which contain backported patches to resolve these issues. After installing this update, the postfix service will be restarted automatically.

1.127. POSTGRESQL

1.127.1. RHSA-2011:0197: Moderate postgresql security update

Updated postgresql packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

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.

PostgreSQL is an advanced object-relational database management system (DBMS).

A stack-based buffer overflow flaw was found in the way PostgreSQL processed certain tokens from an SQL query when the intarray module was enabled on a particular database. An authenticated database user running a specially-crafted SQL query could use this flaw to cause a temporary denial of service (postgres daemon crash) or, potentially, execute arbitrary code with the privileges of the database server. (CVE-2010-4015)

Red Hat would like to thank Geoff Keating of the Apple Product Security team for reporting this issue.

For Red Hat Enterprise Linux 4, the updated postgresql packages contain a backported patch for this issue; there are no other changes.

For Red Hat Enterprise Linux 5, the updated postgresql packages upgrade PostgreSQL to version 8.1.23, and contain a backported patch for this issue. Refer to the PostgreSQL Release Notes for a full list of changes:

http://www.postgresql.org/docs/8.1/static/release.html

For Red Hat Enterprise Linux 6, the updated postgresql packages upgrade PostgreSQL to version 8.4.7, which includes a fix for this issue. Refer to the PostgreSQL Release Notes for a full list of changes:

http://www.postgresql.org/docs/8.4/static/release.html

All PostgreSQL users are advised to upgrade to these updated packages, which correct this issue. If the postgresql service is running, it will be automatically restarted after installing this update.

1.128. POSTGRESQL84

1.128.1. RHSA-2011:0198: Moderate postgresql84 security update

Updated postgresql84 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 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.

PostgreSQL is an advanced object-relational database management system (DBMS).

A stack-based buffer overflow flaw was found in the way PostgreSQL processed certain tokens from an SQL query when the intarray module was enabled on a particular database. An authenticated database user running a specially-crafted SQL query could use this flaw to cause a temporary denial of service (postgres daemon crash) or, potentially, execute arbitrary code with the privileges of the database server. (CVE-2010-4015)

Red Hat would like to thank Geoff Keating of the Apple Product Security team for reporting this issue.

These updated postgresql84 packages upgrade PostgreSQL to version 8.4.7. Refer to the PostgreSQL Release Notes for a full list of changes:

http://www.postgresql.org/docs/8.4/static/release.html

All PostgreSQL users are advised to upgrade to these updated packages, which correct this issue. If the postgresql service is running, it will be automatically restarted after installing this update.

1.129. PROCPS

1.129.1. RHBA-2011:0459: procps bug fix 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. The procps package includes the following commands: ps, free, skill, pkill, pgrep, snice, tload, top, uptime, vmstat, w, watch, and pdwx.

This updated procps package includes fixes for the following bugs:

* The vmstat command, which reports virtual memory statistics, accepted as arguments to its "-S" (size) option the letters "k", "K" or "M". These size identifiers had to be preceded by whitespace, such as in "vmstat -S M". This update removes the whitespace restriction so that the size-representing letter can immediately follow the option; for example, "vmstat -Sk" is now equivalent to "vmstat -S k". (BZ#531439)

* The manual page for the ps command (which displays a snapshot of currently active processes) used a non-standard layout with faulty indentation. With this update, the ps manual page has been modified to match the standard manual page layout. (BZ#564310)

* The vmstat command restricted the length of a device name to 15 character, when, in fact, the device name can be up to 32 characters long. As a result, devices with a 15 and more character names were not displayed when the "vmstat -d" command was issued. With this update, the character limit has been increased to allow device names with up to 32 characters. (BZ#586078)

* Prior to this update, the manual page for the pmap command (which displays a memory map of one or more processes) did not describe the column elements (that is, Address, Kbytes, RSS, Dirty Mode, and Mapping) in the table provided by the "pmap -x" command. With this update, the pmap manual page now provides a short description for each of the aforementioned column elements. (BZ#586116)

* When using the top command (which provides a dynamic real-time view of active processes), a slight inaccuracy in the computing of values in the "%CPU" column caused the displayed values to be higher than 100%. This update fixes this behavior and values displayed in the "%CPU" column can no longer exceed 100%. (BZ#616829)

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

1.130. PSMISC

1.130.1. RHBA-2011:0168: psmisc bug fix update

An updated psmisc package that fixes two bugs is now available for Red Hat Enterprise Linux 5.

The psmisc package contains utilities for managing processes on your system: pstree, killall, and fuser. The pstree command displays a tree structure of all of the running processes on your system. The killall command sends a specified signal (SIGTERM if nothing is specified) to processes identified by name. The fuser command identifies the PIDs of processes that are using specified files or file systems.

This update fixes the following bugs:

* Due to an error in memory allocation, an attempt to kill a process group by using the "killall -g" command could fail. With this update, the memory allocation has been corrected, and the killall utility now works as expected. (BZ#668991)

* Previously, using the fuser command to list processes that use a UDP port failed to produce the expected results. This was caused by an incorrect use of the /proc/net/tcp socket table instead of /proc/net/udp. With this update, the underlying source code has been adjusted to parse the correct socket table, and fuser no longer fails to list processes for UDP ports. (BZ#669309)

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

1.131. PYKICKSTART

1.131.1. RHBA-2011:1022: pykickstart bug fix and enhancement update

An updated pykickstart package that fixes one bug and adds one enhancement is now available for Red Hat Enterprise Linux 5.

The pykickstart package is a python library used to manipulate kickstart files.

This update fixes the following bug:

* Prior to this update, only the first group listed for removal was processed, and only if it was the last line in the %packages section when the group removal syntax was added. With this update, a list of all excluded groups is preserved. Now, all marked package groups are removed, not only the last group. (BZ#577334)

This update also adds the following enhancement:

* By default, anaconda opens a hole in the firewall to allow for Secure Shell (SSH). With this update, the option --no-ssh to the firewall command allows the user to disable this kickstart setting. (BZ#681944)

All pykickstart users are advised upgrade to this updated package, which fix this bug and adds this enhancement.

1.132. PYOPENSSL

1.132.1. RHBA-2011:0483: pyOpenSSL bug fix update

An updated pyOpenSSL package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The pyOpenSSL package provides a high-level wrapper around a subset of the OpenSSL library for the Python programming language.

The update fixes the following bug:

* Previously, an attempt to use the "crypto.X509Extension" class caused the calling application to terminate unexpectedly with a segmentation fault. This update applies a patch that addresses this issue, and using this class no longer causes such applications to crash. (BZ#637398)

All users of pyOpenSSL are advised to upgrade to this updated package, which fixes this bug.

1.133. PYTHON

1.133.1. RHSA-2011:0492: Moderate python security update

Updated python packages that fix multiple security issues 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.

Python is an interpreted, interactive, object-oriented programming language.

A flaw was found in the Python urllib and urllib2 libraries where they would not differentiate between different target URLs when handling automatic redirects. This caused Python applications using these modules to follow any new URL that they understood, including the "file://" URL type. This could allow a remote server to force a local Python application to read a local file instead of the remote one, possibly exposing local files that were not meant to be exposed. (CVE-2011-1521)

A race condition was found in the way the Python smtpd module handled new connections. A remote user could use this flaw to cause a Python script using the smtpd module to terminate. (CVE-2010-3493)

An information disclosure flaw was found in the way the Python CGIHTTPServer module processed certain HTTP GET requests. A remote attacker could use a specially-crafted request to obtain the CGI script's source code. (CVE-2011-1015)

A buffer over-read flaw was found in the way the Python Expat parser handled malformed UTF-8 sequences when processing XML files. A specially-crafted XML file could cause Python applications using the Python Expat parser to crash while parsing the file. (CVE-2009-3720)

This update makes Python use the system Expat library rather than its own internal copy; therefore, users must have the version of Expat shipped with RHSA-2009:1625 installed, or a later version, to resolve the CVE-2009-3720 issue.

All Python users should upgrade to these updated packages, which contain backported patches to correct these issues.

1.134. PYTHON-IMAGING

1.134.1. RHBA-2011:0205: python-imaging bug fix update

An updated python-imaging package that fixes a bug is now available for Red Hat Enterprise Linux 5.

The Python Imaging Library (PIL) adds image processing capabilities to the Python interpreter.

This update fixes the following bug:

* The shebang lines in Python executables have been changed to "#!/usr/bin/python" to ensure the Python interpreter installed in the system is used. (BZ#521304)

All users of python-imaging are advised to upgrade to this updated package, which resolves this issue.

1.135. PYTHON-NUMERIC

1.135.1. RHBA-2011:0508: python-numeric bug fix update

An updated python-numeric package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The python-numeric package is a Python module that provides enhanced support for numerical operations.

This update fixes the following bug:

* Previously, an attempt to use the Numeric.reshape() method to reshape an array into a multi-dimensional array caused Python to terminate unexpectedly with the following error message:

ValueError: total size of new array must be unchanged

With this update, a patch has been applied to address this issue, and the Numeric.reshape() method no longer causes Python to crash. (BZ#703160)

Users are advised to upgrade to this updated python-numeric package, which fixes this bug.

1.136. PYTHON-VIRTINST

1.136.1. RHBA-2011:1054: python-virtinst bug fix and enhancement update

An enhanced python-virtinst package that fixes various bugs and provides an enhancement is now available for Red Hat Enterprise Linux 5.

The python-virtinst utility is a module that helps build and install libvirt-based virtual machines.

This updated python-virtinst package includes fixes for the following bugs:

* A missing "boot-on" parameter caused the installation of a Windows guest to fail due to the reqiured disk device being offline. This problem has been fixed: the "boot=on" value is now among the command line values and the installation successfully completes. (BZ#568294)

* Previously, after a qcow2 image was created using the "qemu-img" command, a virtual machine could not be installed to this image using the "virt-install" command. The "virt-install" command now supports the qcow2 image.(BZ#644271)

In addition, this updated python-virtinst package provides the following enhancement:

* There was a typo in the randomMAC method for the Xen utility defined in the util.py file. The randomly generated MAC addresses incorrectly started with the prefix 00:16:36. This could have caused some tools depending on the expected MAC prefix to not work with guests created by the virt-install tool. This has been fixed and the MAC addresses now correctly start with the prefix 00:16:3E. (BZ#679949)

All users of python-virtinst are advised to upgrade to this updated package, which resolves these bugs and provides this enhancement.

1.137. QUOTA

1.137.1. RHBA-2011:0416: quota bug fix update

An updated quota package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The quota package contains system administration tools for monitoring and limiting user and group disk usage on file systems.

This update fixes the following bug:

* The setquota and edquota utilities provide the "-r" command line option, which allows users to set quotas over the remote procedure call (RPC) protocol. Prior to this update, the usage information for edquota incorrectly stated that this option can be used along with the "-t" and "-T" command line options to set a grace period and grace time. With this update, the usage information has been corrected, and the setquota and edquota utilities have been adapted to report an error when this combination of options is used. (BZ#638578)

All users of quota are advised to upgrade to this updated package, which fixes this bug.

1.138. RDESKTOP

1.138.1. RHSA-2011:0506: Moderate rdesktop security update

An updated rdesktop package that fixes one security issue is now available for Red Hat Enterprise Linux 5 and 6.

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.

rdesktop is a client for the Remote Desktop Server (previously, Terminal Server) in Microsoft Windows. It uses the Remote Desktop Protocol (RDP) to remotely present a user's desktop.

A directory traversal flaw was found in the way rdesktop shared a local path with a remote server. If a user connects to a malicious server with rdesktop, the server could use this flaw to cause rdesktop to read and write to arbitrary, local files accessible to the user running rdesktop. (CVE-2011-1595)

Red Hat would like to thank Cendio AB for reporting this issue. Cendio AB acknowledges an anonymous contributor working with the SecuriTeam Secure Disclosure program as the original reporter.

Users of rdesktop should upgrade to this updated package, which contains a backported patch to resolve this issue.

1.138.2. RHBA-2011:0207: rdesktop bug fix update

An updated rdesktop package that fixes a bug is now available for Red Hat Enterprise Linux 5.

The rdesktop package provides an open source client for Windows NT Terminal Server Edition, and Windows 2000 and Windows 2003 Terminal Services. It supports Remote Desktop Protocol (RDP) in order to remotely present a user's desktop, and does not require any server extensions.

This update fixes the following bug:

* When connecting to a Windows Server 2008 machine, receiving a redirect could cause the rdesktop client to terminate unexpectedly with a segmentation fault. This update applies a patch that fixes this error, and receiving a redirect from Windows Server 2008 no longer causes rdesktop to crash. (BZ#656199)

Users of rdesktop are advised to upgrade to this updated package, which resolves this issue.

1.139. REDHAT-RELEASE

1.139.1. RHEA-2011:0977: redhat-release enhancement update

A new redhat-release package is now available for Red Hat Enterprise Linux 5.7.

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 5.7. (BZ#366331, BZ#666527, BZ#671583, BZ#677386, BZ#695254, BZ#701304, BZ#701692, BZ#702606, BZ#706518, BZ#707649, BZ#708283, BZ#712793)

Users of Red Hat Enterprise Linux 5.7 are advised to install this new package.

1.140. REDHAT-RELEASE-NOTES

1.140.1. RHEA-2011:1064: redhat-release-notes enhancement update

An updated redhat-release-notes package is now available for Red Hat Enterprise Linux 5.7.

The redhat-release-notes package contains licensing information regarding, and identifies the installed version of, Red Hat Enterprise Linux.

This updated redhat-release-notes package reflects changes made for, and contains the Release Notes for, the Red Hat Enterprise Linux 5.7 release.

Users of Red Hat Enterprise Linux 5 are advised to upgrade to this updated redhat-release-notes package, which adds this enhancement.

1.141. RGMANAGER

1.141.1. RHSA-2011:1000: Low rgmanager security, bug fix, and enhancement update

An updated rgmanager package that fixes one security issue, several bugs, and adds multiple enhancements is 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 rgmanager package contains the Red Hat Resource Group Manager, which provides the ability to create and manage high-availability server applications in the event of system downtime.

It was discovered that certain resource agent scripts set the LD_LIBRARY_PATH environment variable to an insecure value containing empty path elements. A local user able to trick a user running those scripts to run them while working from an attacker-writable directory could use this flaw to escalate their privileges via a specially-crafted dynamic library. (CVE-2010-3389)

Red Hat would like to thank Raphael Geissert for reporting this issue.

This update also fixes the following bugs:

* The failover domain "nofailback" option was not honored if a service was in the "starting" state. This bug has been fixed. (BZ#669440)

* PID files with white spaces in the file name are now handled correctly. (BZ#632704)

* The /usr/sbin/rhev-check.sh script can now be used from within Cron. (BZ#634225)

* The clustat utility now reports the correct version. (BZ#654160)

* The oracledb.sh agent now attempts to try the "shutdown immediate" command instead of using the "shutdown abort" command. (BZ#633992)

* The SAPInstance and SAPDatabase scripts now use proper directory name quoting so they no longer collide with directory names like "/u". (BZ#637154)

* The clufindhostname utility now returns the correct value in all cases. (BZ#592613)

* The nfsclient resource agent now handles paths with trailing slashes correctly. (BZ#592624)

* The last owner of a service is now reported correctly after a failover. (BZ#610483)

* The /usr/share/cluster/fs.sh script no longer runs the "quotaoff" command if quotas were not configured. (BZ#637678)

* The "listen" line in the /etc/httpd/conf/httpd.conf file generated by the Apache resource agent is now correct. (BZ#675739)

* The tomcat-5 resource agent no longer generates incorrect configurations. (BZ#637802)

* The time required to stop an NFS resource when the server is unavailable has been reduced. (BZ#678494)

* When using exclusive prioritization, a higher priority service now preempts a lower priority service after status check failures. (BZ#680256)

* The postgres-8 resource agent now correctly detects failed start operations. (BZ#663827)

* The handling of reference counts passed by rgmanager to resource agents now works properly, as expected. (BZ#692771)

As well, this update adds the following enhancements:

* It is now possible to disable updates to static routes by the IP resource agent. (BZ#620700)

* It is now possible to use XFS as a file system within a cluster service. (BZ#661893)

* It is now possible to use the "clustat" command as a non-root user, so long as that user is in the "root" group. (BZ#510300)

* It is now possible to migrate virtual machines when central processing is enabled. (BZ#525271)

* The rgmanager init script will now delay after stopping services in order to allow time for other nodes to restart them. (BZ#619468)

* The handling of failed independent subtrees has been corrected. (BZ#711521)

All users of Red Hat Resource Group Manager are advised to upgrade to this updated package, which contains backported patches to correct these issues and add these enhancements.

1.141.2. RHBA-2011:0509: rgmanager bug fix update

An updated rgmanager package that fixes two bugs is now available for Red Hat Enterprise Linux 5.

The rgmanager package contains 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 fixes the following bugs:

* Prior to this update, the fs.sh agent incorrectly attempted to run the quotaoff command even when disk quotas were not enabled. Under certain circumstances, this may have caused the agent to stop responding during a service shutdown or relocation. This update applies a patch that prevents the fs.sh agent from running the quotaoff command when disk quotas are not enabled. As a result, the agent no longer stops responding during a service shutdown or relocation. (BZ#694731)

* Due to an error in the reference count handling mechanism, previous version of the Red Hat Resource Group Manager failed to unmount a partition when it was not used by any service. With this update, the reference count handling for clustered file systems has been corrected, and unused partitions are now unmounted as expected. (BZ#701233)

All users of Red Hat Resource Group Manager are advised to upgrade to this updated package, which fixes these bugs.

1.142. RHN-CLIENT-TOOLS

1.142.1. RHBA-2011:0997: rhn-client-tools bug fix and enhancement update

Updated rhn-client-tools packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

RHN Client Tools provides programs and libraries that allow a system to receive software updates from Red Hat Network (RHN) or Red Hat Network Satellite.

This update fixes the following bugs:

* Previously, when sending a hardware profile to RHN or Red Hat Network Satellite, the rhn-profile-sync command did not report virtual IP addresses if they were configured on an active network interface. This was caused by an incorrect use of the ethtool.get_devices() function. The underlying source code has been modified to use the ethtool.get_active_devices() function instead, and rhn-profile-sync now works as expected. (BZ#624748)

* After a failed login into RHN, the rhn_register utility still showed a busy cursor. This happened even after pressing "Ok" or "Back" to acknowledge the error message. Now, a normal arrow cursor appears. (BZ#649208)

* The manual page was missing for the rhn-channel utility. This problem has been fixed and the rhn-channel(8) manual page is now included. (BZ#651778)

* When removing or adding a wrong channel, the rhn-channel utility incorrectly reported successfully completed operation. This has been fixed: rhn-channel now informs, that the wrong channel cannot be added or removed. (BZ#651790)

* When used with an incorrect option combination, the rhn-channel program failed with a traceback report.The report has been replaced by a simple, informative error message. (BZ#651858)

* Previously, the rhnreg_ks utility failed with a traceback report, when users tried to run rhnreg_ks on clients using Internet Protocol version 6 (IPv6). The problem has been solved and rhnreg_ks now works properly. (BZ#665013)

* The file /usr/share/application/rhn_register.desktop was missing in the previous version of the rhn-setup-gnome package. Therefore, there was a menu item missing in the graphical user interface of the rhn_register utility. This problem has been fixed: the file is now included and the utility works as expected. (BZ#688627)

* Previously, the Tab key did not work to select items in one of the screens of the firstboot utility. This prevented users from using a keyboard and they had to use a mouse instead. This problem has been solved: both a mouse and a keyboard can now be used. (BZ#707938)

As well, this update adds the following enhancements:

* This update sets the firstboot registration method by default to RHN Classic. (BZ#694908)

* Previously, when changing a channel subscription, the rhn-channel program accepted a username and a password only as parameters on the command line. As a consequence, other people could have read personal data. Now, users are prompted for the username and the password if they are not entered as parameters. (BZ#641029)

* Names related to the new way of subscriptions have been changed in the rhn_register utility. This applies to changing the subscription title from Red Hat Network to the new Red Hat Network Classic or Red Hat Network Satellite. Also, warning and informational messages were changed or added in dependency on a used subscription method. Subscription Manager is now introduced as an alternative for registration. (BZ#675217, BZ#707288, BZ#676916)

* Due to the change of the RHN subscription methods, several texts in manual pages were changed. This applies to the rhn_register and rhnreg_ks utilities, where Red Hat Network has been replaced with Red Hat Network Classic. (BZ#675218)

Users are advised to upgrade to these updated rhn-client-tools packages, which fix these bugs and add these enhancements.

1.143. RHNLIB

1.143.1. RHEA-2011:0996: rhnlib enhancement update

An updated rhnlib package that adds one enhancement is now available for Red Hat Enterprise Linux 5.

The rhnlib package consists of a collection of Python modules used by the Red Hat Network (RHN) software.

This update adds the following enhancement:

* Two new functions have been added in order to allow the upcoming support for internationalized domain names (IDN) in the future releases of yum-rhn-plugin, Red Hat Network Tools, and Red Hat Network Satellite. (BZ#684813)

All users of rhnlib are advised to upgrade to this updated package, which adds this enhancement.

1.144. RHNSD

1.144.1. RHBA-2011:1043: rhnsd bug fix update

An updated rhnsd package that fixes two bugs is now available for Red Hat Enterprise Linux 5.

The rhnsd package includes 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.

This update fixes the following bugs:

* Previously, it was not possible to reload the Red Hat Update Agent (rhnsd) service configuration properly. This was due to the bug in reading the service configuration during the service startup. The bug has been fixed in this update so that the service configuration can now be reloaded as expected. (BZ#502234)

* Previously, the Red Hat Update Agent (rhnsd) failed to find the systemid file if the file was stored in a non-standard location. The fix for the bug has been provided in this update so that the systemid file location is now determined from reading the /etc/sysconfig/rhn/up2date file. (BZ#524886)

All users requiring rhnsd are advised to upgrade to this updated package which fixes these bugs.

1.145. RSYNC

1.145.1. RHSA-2011:0999: Moderate rsync security, bug fix, and enhancement update

An updated rsync package that fixes one security issue, several bugs, and adds enhancements is 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.

rsync is a program for synchronizing files over a network.

A flaw was found in the way the rsync daemon handled the "filter", "exclude", and "exclude from" options, used for hiding files and preventing access to them from rsync clients. A remote attacker could use this flaw to bypass those restrictions by using certain command line options and symbolic links, allowing the attacker to overwrite those files if they knew their file names and had write access to them. (CVE-2007-6200)

Note: This issue only affected users running rsync as a writable daemon: "read only" set to "false" in the rsync configuration file (for example, "/etc/rsyncd.conf"). By default, this option is set to "true".

This update also fixes the following bugs:

* The rsync package has been upgraded to upstream version 3.0.6, which provides a number of bug fixes and enhancements over the previous version. (BZ#339971)

* When running an rsync daemon that was receiving files, a deferred info, error or log message could have been sent directly to the sender instead of being handled by the "rwrite()" function in the generator. Also, under certain circumstances, a deferred info or error message from the receiver could have bypassed the log file and could have been sent only to the client process. As a result, an "unexpected tag 3" fatal error could have been displayed. These problems have been fixed in this update so that an rsync daemon receiving files now works as expected. (BZ#471182)

* Prior to this update, the rsync daemon called a number of timezone-using functions after doing a chroot. As a result, certain C libraries were unable to generate proper timestamps from inside a chrooted daemon. This bug has been fixed in this update so that the rsync daemon now calls the respective timezone-using functions prior to doing a chroot, and proper timestamps are now generated as expected. (BZ#575022)

* When running rsync under a non-root user with the "-A" ("--acls") option and without using the "--numeric-ids" option, if there was an Access Control List (ACL) that included a group entry for a group that the respective user was not a member of on the receiving side, the "acl_set_file()" function returned an invalid argument value ("EINVAL"). This was caused by rsync mistakenly mapping the group name to the Group ID "GID_NONE" ("-1"), which failed. The bug has been fixed in this update so that no invalid argument is returned and rsync works as expected. (BZ#616093)

* When creating a sparse file that was zero blocks long, the "rsync --sparse" command did not properly truncate the sparse file at the end of the copy transaction. As a result, the file size was bigger than expected. This bug has been fixed in this update by properly truncating the file so that rsync now copies such files as expected. (BZ#530866)

* Under certain circumstances, when using rsync in daemon mode, rsync generator instances could have entered an infinitive loop, trying to write an error message for the receiver to an invalid socket. This problem has been fixed in this update by adding a new sibling message: when the receiver is reporting a socket-read error, the generator will notice this fact and avoid writing an error message down the socket, allowing it to close down gracefully when the pipe from the receiver closes. (BZ#690148)

* Prior to this update, there were missing deallocations found in the "start_client()" function. This bug has been fixed in this update and no longer occurs. (BZ#700450)

All users of rsync are advised to upgrade to this updated package, which resolves these issues and adds enhancements.

1.146. RSYSLOG

1.146.1. RHBA-2011:0484: rsyslog bug fix update

Updated rsyslog packages that fix a bug are now available for Red Hat Enterprise Linux 5.

The rsyslog packages provide an enhanced, multi-threaded syslog daemon that supports MySQL, syslog/TCP, RFC 3195, permitted sender lists, filtering on any message part, and fine grained output format control.

This update fixes the following bug:

* The rsyslog bug fix update for Red Hat Enterprise Linux 5.5, which is advisory RHBA-2010:0213, contained an enhancement that increased the number of clients that rsyslog was able to handle. However, an issue with the build tool chain resulted in the source code patch failing to apply, with the results that large numbers of clients could have caused rsyslogd to crash due to a segmentation fault. The patch has been successfully applied with this update, and rsyslogd is now able to handle a large number of clients without crashing. (BZ#692954)

All users of rsyslog are advised to upgrade to these updated packages, which fixes this bug.

1.147. RUBY

1.147.1. RHSA-2011:0909: Moderate ruby security update

Updated ruby packages that fix multiple security issues 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.

Ruby is an extensible, interpreted, object-oriented, scripting language. It has features to process text files and to do system management tasks.

A flaw was found in the way large amounts of memory were allocated on 64-bit systems when using the BigDecimal class. A context-dependent attacker could use this flaw to cause memory corruption, causing a Ruby application that uses the BigDecimal class to crash or, possibly, execute arbitrary code. This issue did not affect 32-bit systems. (CVE-2011-0188)

A race condition flaw was found in the remove system entries method in the FileUtils module. If a local user ran a Ruby script that uses this method, a local attacker could use this flaw to delete arbitrary files and directories accessible to that user via a symbolic link attack. (CVE-2011-1004)

It was found that WEBrick (the Ruby HTTP server toolkit) did not filter terminal escape sequences from its log files. A remote attacker could use specially-crafted HTTP requests to inject terminal escape sequences into the WEBrick log files. If a victim viewed the log files with a terminal emulator, it could result in control characters being executed with the privileges of that user. (CVE-2009-4492)

A cross-site scripting (XSS) flaw was found in the way WEBrick displayed error pages. A remote attacker could use this flaw to perform a cross-site scripting attack against victims by tricking them into visiting a specially-crafted URL. (CVE-2010-0541)

A flaw was found in the method for translating an exception message into a string in the Exception class. A remote attacker could use this flaw to bypass safe level 4 restrictions, allowing untrusted (tainted) code to modify arbitrary, trusted (untainted) strings, which safe level 4 restrictions would otherwise prevent. (CVE-2011-1005)

Red Hat would like to thank Drew Yao of Apple Product Security for reporting the CVE-2011-0188 and CVE-2010-0541 issues.

All Ruby users should upgrade to these updated packages, which contain backported patches to resolve these issues.

1.148. S390UTILS

1.148.1. RHBA-2011:1021: s390utils bug fix and enhancement update

An updated s390utils package that fixes various bugs and adds two enhancements is now available for Red Hat Enterprise Linux 5.

The s390utils package contains utilities related to Linux for the IBM System z architecture.

This update fixes the following bugs:

* Prior to this update, the format 7 label written by the fdasd and dasdfmt utilities was incorrect. Consequent to this, backups of Linux on System z disks from z/OS did not work when the disk was not fully partitioned. This update adapts the libvtoc library to make sure that both fdasd and dasdfmt now write the format 7 label correctly. As a result, such backups now work as expected. (BZ#649966)

* When the previous version of the cpuplugd service exited, it incorrectly changed /proc/sys/vm/cmm_pages to 0 regardless of its previous value. Additionally, when the values of cmm_pages and cmm_inc were equal, cmm_pages failed to reach a cmm_min of 0 during runtime. This update adapts the underlying source code to retain the value of /proc/sys/vm/cmm_pages and evaluate cmm_min correctly. (BZ#658273)

* The previous version of the lsluns utility failed to report LUNs from the SAN Volume Controller (SVC). This update changes the strategy of this utility to determine whether LUN 0 or the WLUN is already available. Now, if none of the LUNs is available, LUN 0 is tried first, and if it fails, the WLUN is tried next. As a result, the lsluns utility reports LUNs from the SVC as expected. (BZ#659827)

* Previously, the lsluns utility did not accept uppercase letters for hex digits in an FCP device identifier or WWPN. This error no longer occurs, and lsluns now accepts both uppercase and lowercase letters. (BZ#660359)

* Prior to this update, the cpuplugd service did not evaluate rules correctly when the multiplication (that is, *) was used. This update applies a patch that addresses this issue so that such rules are now evaluated correctly. (BZ#693366)

* Previously, the cmsfs utilities crashed when they were used on file systems with block sizes different from the underlying device. Consequently, users had to work around the issue by creating a file system with the same block size as the device. With this update, the cmsfs utilities now report the mismatch in block sizes but still work. (BZ#696149)

* Due to an error in the option parser, the previous version of the ziomon utility incorrectly accepted

the "--output" command line option instead of "--outfile". Consequently, an attempt to run the utility with the "--outfile" option as specified in the documentation failed. This update corrects the option parser to accept the "--outfile" option as described in the documentation. (BZ#697479)

* Previously, mounting the debugfs file system in a directory other than /sys/kernel/debug caused the ziomon utility to fail with an error. This update adapts the underlying source code to verify the debugfs mount path, resolving this issue. (BZ#700687)

As well, this update adds the following enhancements:

* This update introduces an application programming interface (API) to determine the status of a direct access storage device (DASD), and adapts the tunedasd utility to provide the "-Q" (or "--query_reserve") command line option, which allows users to write this information to standard output. (BZ#651142)

* This update adds a new configuration option, "DELAY_MINUTES", to the /etc/sysconfig/dumpconf file. When specified, this option allows a user to delay the activation of the dumpconf service to prevent possible re-IPL loops. (BZ#651168)

All users of s390utils are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

1.149. SABAYON

1.149.1. RHBA-2011:0504: sabayon bug fix update

Updated sabayon packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The sabayon packages provide the Sabayon tool which helps to maintain or change the GNOME desktop default behavior. These packages contain the graphical tools which a system administrator uses to manage Sabayon profiles.

This update fixes the following bug:

* Previously, Sabayon used /usr/bin/env to locate python on the system. Due to this behavior, unexpected errors occurred when users set search paths to their own copy of Python which was not fully compatible with the required python version for Sabayon. With this update, Sabayon uses /usr/bin/python. Now, Sabayon works as expected. (BZ#456928)

All Sabayon users are advised to upgrade to these updated packages, which fix this bug.

1.150. SAMBA

1.150.1. RHSA-2011:0305: Important samba security update

Updated samba packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

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.

Samba is a suite of programs used by machines to share files, printers, and other information.

A flaw was found in the way Samba handled file descriptors. If an attacker were able to open a large

number of file descriptors on the Samba server, they could flip certain stack bits to "1" values, resulting in the Samba server (smbd) crashing. (CVE-2011-0719)

Red Hat would like to thank the Samba team for reporting this issue.

Users of Samba are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing this update, the smb service will be restarted automatically.

1.151. SAMBA3X

1.151.1. RHSA-2011:0306: Important samba3x security update

Updated samba3x 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 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.

Samba is a suite of programs used by machines to share files, printers, and other information.

A flaw was found in the way Samba handled file descriptors. If an attacker were able to open a large number of file descriptors on the Samba server, they could flip certain stack bits to "1" values, resulting in the Samba server (smbd) crashing. (CVE-2011-0719)

Red Hat would like to thank the Samba team for reporting this issue.

Users of Samba are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing this update, the smb service will be restarted automatically.

1.151.2. RHBA-2011:1007: samba3x bug fix update

Updated samba3x packages that fix multiple bugs are now available for Red Hat Enterprise Linux 5.

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).

This update fixes the following bugs:

* Prior to this update, the smbd service unexpectedly changed file permissions while renaming files, although the permissions change was not requested by the Samba client. This erroneous behavior has been fixed in this update and no longer occurs. (BZ#661311)

* When trying to access resources on Samba server with an invalid password, any further attempt to log in after the unsuccessful attempt, no matter what was the account or Samba shares, failed with the "session setup failed: NT code 0x1c010002" error message. This bug has been fixed in this update so that further attempts to log in no longer fail, as expected. (BZ#716961)

* Prior to this update, it was not possible to join a Samba machine in the Windows Server 2008 Active Directory (Active Directory Domain Services) if using credentials from a trusted domain. This bug has been fixed in this update so that it is now possible to join a Samba machine in the Windows Server 2008 Active Directory, as expected. (BZ#713552)

* When joining a Windows domain, when an attempt to list all the users with "wbinfo" and "getent" records was made, there was no output provided although it was expected. This unintended behavior

has been fixed in this update so that issuing a 'getent passwd "[GROUPNAME]\[username]"' command for all valid users and groups works, as expected. (BZ#679066)

* When changing printer settings on a Windows client for printers shared via a Samba Print Server or CUPS, these settings were not saved properly. This bug has been fixed in this update so that the printer settings are now saved properly, as expected. (BZ#698400)

* When there was a large number of groups and users, if winbind attempted to continue after resolving the first 250 groups, winbind terminated unexpectedly and produced a core dump. This bug has been fixed in this update so that winbind now works as expected when resolving groups. (BZ#704279)

* The smbclient program incorrectly guessed the server principal if a user and server were not in the same Kerberos 5 (krb5) realm and the server's short name was used. As a result, connection to the server failed. This bug has been fixed in this update so that connection to the server now works as expected. (BZ#701661)

* Adding and removing printers with CUPS was not correctly handled by Samba if the "load printers = yes" option was set. Furthermore, error messages emitted by CUPS to Samba were not handled correctly. Also, trying to set the "printcap name = /etc/printcap" option in order to avoid performance penalties when using CUPS with a large number of printers and clients was not working properly. Finally, parsing a printcap file was not working as expected. The aforementioned problems have been fixed in this update and no longer occur. (BZ#701975)

* Samba was not able to receive printer's "location" attribute from CUPS. As a result, it was not possible to view printer's description while browsing printers that were available on the system. This bug has been fixed in this update so that the "location" attribute is now received properly by Samba, as expected. (BZ#702039)

* The mount.cifs(8) man page did not contain a description for the "--nounix" option. This has been fixed in this update by adding the missing description to the man page. (BZ#621686)

* Prior to this update, there were certain inconsistencies between the available options described in the wbinfo(1) man page and the output of the "wbinfo --help" command. The majority of these inconsistencies has been fixed in this update. (BZ#679086)

All users of samba3x are advised to upgrade to these updated packages, which fix these bugs.

1.152. SCIM

1.152.1. RHBA-2011:0355: scim bug fix update

Updated scim packages that fix two bugs are now available for Red Hat Enterprise Linux 5.

The Smart Common Input Method (SCIM) project provides an input method user interface, and a development platform for input method development.

This update fixes the following bugs:

* When using the SCIM Input Method Setup utility to adjust the global setup of IMEngine modules, clicking the "Disable All" button failed to activate the "Apply" button. This rendered users unable to confirm their changes, and one of the items had to be manually selected and deselected to work around this problem. With this update, a patch has been applied to address this issue, and clicking the "Disable All" button now always allows users to click the "Apply" button as expected. (BZ#493809)

* When an application window is opened, SCIM creates a 1x1 window in the background. Prior to this update, this 1x1 window was not properly destroyed when the application window was closed in a non-

standard way (for example, due to a crash or upon receiving the SIGKILL signal). To prevent unnecessary memory consumption, this update adapts the underlying source code to ensure the 1x1 windows are destroyed as expected. (BZ#664464)

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

1.153. SCREEN

1.153.1. RHBA-2011:0401: screen bug fix update

An updated screen package that fixes two bugs is now available for Red Hat Enterprise Linux 5.

The screen utility allows multiple logins on a single terminal. This is especially useful for users who connect to a remote machine or are connected using a terminal that does not provide this functionality, but want to use more than one login.

This update fixes the following bugs:

* The default configuration file contains several tweaks for the xterm terminal emulator, such as displaying the list of windows in the title bar. However, due to the strict use of "xterm" in patterns to match the terminal name, these options were not applied to other xterm variants like xterm-256color or xterm-88color. This update corrects the relevant patterns to match all xterm names, resolving this issue. (BZ#474064)

* Previously, the default configuration disabled the use of the "h" key. Consequent to this, pressing the "Ctrl+a h" key combination to write a printed version of the current window to a file did not work. With this update, the "bind h" option has been removed from the default configuration file, and the above key combination now works as expected. (BZ#521824)

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

1.154. SCSI-TARGET-UTILS

1.154.1. RHSA-2011:0332: Important scsi-target-utils security update

An updated scsi-target-utils package that fixes one security issue is now available for Red Hat Enterprise Linux 5 and 6.

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.

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.

A double-free flaw was found in scsi-target-utils' tgtd daemon. A remote attacker could trigger this flaw by sending carefully-crafted network traffic, causing the tgtd daemon to crash. (CVE-2011-0001)

Red Hat would like to thank Emmanuel Bouillon of NATO C3 Agency for reporting this issue.

All scsi-target-utils users should upgrade to this updated package, which contains a backported patch to correct this issue. All running scsi-target-utils services must be restarted for the update to take effect.

1.154.2. RHBA-2011:1049: scsi-target-utils bug fix and enhancement update

An updated scsi-target-utils package that fixes multiple bugs and adds one enhancement is now available for Red Hat Enterprise Linux 5.

The SCSI target package contains the daemon and tools to setup iSCSI and iSER targets.

This update fixes the following bugs:

* Prior to this update, there was a bug in the "tgt-setup-lun" command that caused a target to be deleted if an invalid Logical Unit Number (LUN) was added. The problem has been resolved in this update so that "tgt-setup-lun" now works as expected and the target is not deleted. (BZ#695867)

* Prior to this update, there was a bug in the iscsid and tgtd daemons that caused the system log to be filled with the "iscsid: semop down failed" and "tgtd: semop up failed" error messages while starting and stopping the respective services in a particular order. The bug has been fixed in this update so that no error messages from iscsid and tgtd are now written in the system log. (BZ#676804)

* Prior to this update, there was a problem with using very large (more than 2TB in size) hard disks with iSCSI. As a result, the iSCSI initiator failed with "very big device. try to use READ CAPACITY(16)" and "unsupported sector size" error messages. This bug has been fixed in this update so that using such hard disks with iSCSI now works as expected. (BZ#674394)

* Prior to this update, the iSCSI initiator on Windows Server 2003 was not able to use Logical Unit Numbers (LUNs) provided by the tgtd daemon on Linux. It did not recognize simultaneous Linux SCSI Target Framework (STGT) LUNs provided by the same STGT target. This bug has been fixed in this update so that the iSCSI initiator is now able to use the LUNs as expected. (BZ#560534)

As well, this update adds the following enhancement:

* This update adds support for a read-only target by setting the "--params readonly=1" option with the "tgtadm" command, or by setting the "readonly 1" and "allow-in-use yes" options in the /etc/tgt/targets.conf file. (BZ#695870)

All users requiring scsi-target-utils should upgrade to this updated package, which fixes these bugs and adds this enhancement.

1.155. SED

1.155.1. RHBA-2011:0397: sed bug fix update

An updated sed package that fixes two bugs is now available for Red Hat Enterprise Linux 5.

Sed is a stream or batch (non-interactive) editor. Sed takes text as input, performs an operation or set of operations on the text, and outputs the modified text.

This update fixes the following bugs:

* Due to an error in a symbolic link resolution, an attempt to use in-place substitution (that is, the "-i" command line option) with a symbolic link caused sed to fail with the following error:

sed: ck_follow_symlink: couldn't lstat [symbolic_link]/[original_file]: Not a directory

With this update, when a symbolic link is supplied, sed determines the original file path correctly. As a result, using the in-place substitution on symbolic links now works as expected. (BZ#490473)

* Previously, when an input stream contained a wide character that ended with U+005C (that is, the '\' character), sed failed to process it and reported a syntax error. This update applies an upstream patch that ensures the wide characters are now processed as expected. Additionally, this update also prevents sed from entering an infinite loop while handling incomplete string sequences. (BZ#527427)

All users of sed are advised to upgrade to this updated package, which fixes these bugs.

1.156. SELINUX-POLICY

1.156.1. RHBA-2011:1069: selinux-policy bug fix and enhancement update

Updated selinux-policy packages that fix several bugs and add two enhancements are now available for Red Hat Enterprise Linux 5.

IMPORTANT

This update was released as errata RHBA-2011:1069 — selinux-policy bug fix and enhancement update.

The selinux-policy packages contain the rules that govern how confined processes run on the system.

Bug Fixes:

BZ#610812

Due to an incorrect SELinux policy, SELinux did not allow **FreeRADIUS** to disable storing core dump files upon a failure. This update applies a backported patch that addresses this issue, and **FreeRADIUS** can now be configured not to create core dumps as expected.

BZ#632573

Previously, when a leaked file descriptor was detected during a system update, an Access Vector Cache (AVC) message was written to the audit log. With this update, the relevant SELinux policy has been added to prevent SELinux from reporting file descriptors leaked during a system update.

BZ#651609

When running in enforcing mode, SELinux did not allow the **clustat** utility to bind to a reserved port. This update adapts the SELinux rules to permit such connection, so that **clustat** is now able to bind to the required port as expected.

BZ#657571

Prior to this update, the SELinux Multi-Level Security (MLS) policy incorrectly prevented the **modprobe** utility from sending the **SIGNULL** signal to all processes. With this update, the relevant policy has been fixed, and SELinux no longer prevents **modprobe** from sending **SIGNULL** to all processes.

BZ#662677

When **Samba** is configured to run as a Windows Internet Name Server (WINS) that is integrated to a Name Service Switch (NSS), programs that resolve a NetBIOS name require access to the **/var/cache/samba/unexpected.tdb** file. Previously, SELinux incorrectly denied this access. This update adapts the relevant SELinux policy to allow this access, and programs resolving a NetBIOS name are now able to access this file as expected.

BZ#666513

Previous versions of the seliux-policy packages did not provide a SELinux policy for the `/var/spool/rsyslog/` directory. With this update, this policy has been added.

BZ#667692

When the `utmp` option in the `/etc/samba/smb.conf` configuration file is set to `yes`, **Samba** records sessions in the `utmp` and `wtmp` files. Prior to this update, the SELinux policy did not allow the `smbd` daemon to write to the `wtmp` file. With this update, the SELinux policy has been corrected, so that **Samba** is now allowed to work as expected.

BZ#672289

When running in enforcing mode, SELinux did not allow the `net` utility to create a Kerberos keytab file when the system was joined to a Windows 2003 Active Directory domain. This update corrects this error, and SELinux no longer prevents the `net` utility from creating a Kerberos keytab file.

BZ#672540

Prior to this update, an attempt to use the System Security Services Daemon (SSSD) with an LDAP domain connected to an OpenLDAP server over the Transport Layer Security (TLS) protocol caused various AVC messages to be written to the audit log. This update applies a backported patch that resolves this issue, so that no unnecessary AVC messages are recorded.

BZ#674452

The `rsyslogd` tool allows a user to change the maximum number of open file descriptors by adding the `$MaxOpenFiles` directive to the `/etc/rsyslog.conf` file. Previously, an attempt to use this directive to set a number that is larger than the default value failed, because SELinux prevented `rsyslogd` from accessing `setrlimit`. This update corrects the relevant policy to allow this access, so that the `rsyslogd` tool is now able to increase the maximum number of open file descriptors as expected.

BZ#674689

In order to perform its job, the `pyzor` client requires access to certain files in users' home directories. Prior to this update, SELinux did not allow `pyzor` to access these files if the home directories were located on an NFS mount point. With this update, SELinux no longer denies `pyzor` access to NFS-mounted home directories, allowing it to work correctly.

BZ#678496

Due to missing SELinux policies, various AVC messages may have been reported when attempting to start the `pulse` or `ipvsadm` service. This update adds the relevant policies to make sure these services can be started as expected.

BZ#689960

For debugging purposes, **Openswan** allows a user to specify a directory in which to store a core dump file in case the `pluto` service crashes. Prior to this update, running SELinux in enforcing mode rendered **Openswan** unable to create such a core dump. With this update, the relevant policy has been corrected, and SELinux no longer prevents **Openswan** from creating core dump files.

BZ#693723

The `sshd` service, `ssh` client, and other SSH-aware utilities need to read data from the `/dev/random` and `/dev/urandom` devices. Prior to this update, SELinux may have incorrectly prevented these programs from accessing these devices. This update adapts the SELinux policy so

that these utilities are able to read data from both `/dev/random` and `/dev/urandom` as expected.

BZ#694865

Due to an incorrect SELinux policy, the **Pyzor** spam filtering system was incorrectly denied access to configuration files located in the `/etc/` directory. This update corrects the SELinux policy to make sure **Pyzor** is no longer prevented from accessing its configuration files.

BZ#697804

With SELinux running in enforcing mode, any communication via the Stream Control Transmission Protocol (SCTP) was denied. With this update, the relevant SELinux policy has been adapted to allow the SCTP communication.

BZ#698043

Prior to this update, restarting the `vsftpd` service by using the `service vsftpd restart` command caused an AVC message to be written to the audit log. With this update, SELinux rules have been added to address this issue, and restarting the `vsftpd` service no longer produces AVC messages.

BZ#698257

With SELinux enabled, running the `named` service in a chroot environment rendered it unable to update log files. This error has been fixed, and SELinux no longer prevents `named` from updating the log files.

BZ#703458

Previously, the SELinux Multi-Level Security (MLS) policy incorrectly prevented the `lsusb` command from producing the expected results. This update corrects the relevant policy so that the command works as expected.

BZ#703482

Previously, the SELinux Multi-Level Security (MLS) policy incorrectly prevented the `kpartx -x` command from producing the expected results. This update corrects the relevant policy so that the command works as expected.

BZ#703714

Due to an incorrect SELinux policy, when the **OpenAIS Standards-Based Cluster Framework** was started, various AVC messages were written to the audit log, and the `openais` service was unable to use UDP port 5404. This error has been fixed, the relevant SELinux policy has been corrected, and the `openais` service now works as expected.

BZ#704690

Previous versions of the selinux-policy packages were missing SELinux rules for the `syslog-ng` syslog server. With this update, these rules have been added.

BZ#705327

Previously, using the `arping` utility on an IBM System z machine incorrectly caused an AVC message to be written to the audit log. This update corrects the relevant SELinux policy, and running `arping` no longer produces unnecessary AVC messages.

BZ#707101

Prior to this update, SELinux incorrectly prevented the **clamav-milter** utility to from opening a socket, causing it to terminate with an error. With this update, this error has been fixed, and **clamav-milter** can now be used as expected.

BZ#707139

With SELinux running in enforcing mode, the Apache HTTP Server may have been unable to use the **worker** Multi-Processing Module (MPM). This update applies a backported patch that adds the **httpd_execmem** boolean. As a result, SELinux no longer prevents the Apache HTTP Server from loading the **worker** MPM.

BZ#708986

Prior to this update, the SELinux Multi-Level Security (MLS) policy prevented the **user_u** and **staff_u** SELinux users from running the **ssh-keygen** utility. This update fixes the relevant policy, and both **user_u** and **staff_u** users are now able to run **ssh-keygen** as expected.

BZ#709045

Previously, the SELinux Multi-Level Security (MLS) policy incorrectly prevented the **crontab -l** command from producing the expected results. This update corrects the relevant policy so that the command works as expected.

BZ#711725

Prior to this update, the SELinux Multi-Level Security (MLS) policy prevented the **iprinit**, **iprdump**, and **iprupdate** services from working correctly. With this update, this error no longer occurs, and the aforementioned services are able to work as expected.

BZ#713797

Due to an error in SELinux rules, running SELinux in enforcing mode rendered the **clustat** utility unable to connect to a cluster port. With this update, the SELinux rules have been updated to permit such connection, resolving this issue.

BZ#714960

Prior to this update, the **.k5login** files in the users' home directories were labeled with a wrong security context, which caused SELinux to incorrectly prevent the **krb5_child** process from accessing these files. With this update, the security context of the **.k5login** files has been corrected so that **krb5_child** is no longer denied access to these files.

Enhancements:

BZ#662097

This update introduces the **squid_selinux**(8) manual page, which provides detailed documentation of the SELinux policy for the **squid** daemon.

BZ#671498

This update adds a new security context for devices in the **/dev/hpilo/** directory, which provide an interface to the HP Integrated Lights-Out (iLO) remote management functionality.

All users of SELinux are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

1.156.2. RHBA-2011:0481: selinux-policy bug fix update

Updated selinux-policy packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The selinux-policy packages contain the rules that govern how confined processes run on the system.

This update fixes the following bug:

* The sshd service, ssh clients, and other SSH-aware utilities require access to the /dev/random and /dev/urandom random number generators. Prior to this update, SELinux incorrectly prevented the ssh-keygen utility from accessing the /dev/random device. This update adapts SELinux policies to allow this access, and ssh-keygen is now able to read data from /dev/random as expected. (BZ#694048)

All users are advised to upgrade to these updated packages, which fix this bug.

1.157. SHADOW-UTILS

1.157.1. RHBA-2011:0823: shadow-utils bug fix update

An updated shadow-utils package that fixes three bugs is now available for Red Hat Enterprise Linux 5.

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.

This update fixes the following bugs:

* When a new user is created, the content of the /etc/skel/ directory is copied to the user's home directory. Previously, an attempt to copy these files and directories from a file system with the support for access control lists (ACLs) enabled to a file system with ACLs disabled failed with an error, and some files were not copied. With this update, a patch has been applied to address this issue, and when a new user is created, the content of the /etc/skel/ directory is now successfully copied without an error. (BZ#690829)

* Due to incorrect handling of large user and group identifiers (that is, UIDs and GIDs) on 32-bit systems, the pwconv and pwunconv utilities changed all identifiers greater than 2147483647 to this value. With this update, the underlying source code has been adapted to ensure the pwconv and pwunconv utilities no longer alter the GIDs and UIDs. (BZ#690830)

* Previously, the faillog utility executed command line options as they were passed instead of parsing all options first. This update applies a patch that corrects the utility to parse all command line options before executing the commands. (BZ#690831)

All users of shadow-utils are advised to upgrade to this updated package, which fixes these bugs.

1.158. SOS

1.158.1. RHBA-2011:1028: sos bug fix and enhancement update

An updated sos package that fixes several bugs and adds various enhancements is now available for Red Hat Enterprise Linux 5.

The sos package contains a set of tools that gather information from system hardware, logs and configuration files. The information can then be used for diagnostic purposes and debugging.

This updated sos package provides fixes for the following bugs:

* The sos utility did not include the rsyslog.conf file in sos reports. This update adds the rsyslog plug-in, which adds rsyslog.conf to the reports. (BZ#548616)

* The hardware.py plug-in of the up2date client used an incorrect path to the hardware.py script. This update corrects the path. (BZ#572353)

* The rhn plug-in failed to include the squid logs from RHN proxy servers. This occurred because the plug-in failed to identify such servers. This update adapts the underlying code and the squid logs from RHN proxy servers are included in sos reports as expected. (BZ#590389)

* Prior to this update, sos reports did not include the log files defined in the syslog and rsyslog configuration files. This happened because the utility did not search the files for log file definitions. This update adds the respective code and sos collects all user-defined log files specified in rsyslog.conf or syslog.conf. (BZ#596970)

* The Certificate system plug-in did not collect logs from Red Hat Certificate System 8.0. With this update, dogtag.py for Red Hat Certificate System 8.0 has been added and sos collects logs from Red Hat Certificate System 8.0, as expected. (BZ#635966)

* On IBM S/390 architecture, outputs from the parted and dumpe2fs utilities were not included in sos reports. This bug has been fixed and data retrieved from both utilities are now included in sos reports. (BZ#645507)

* The selinux plug-in did not gather the /etc/sysconfig/selinux file. This is now fixed and the file is included in the reports of the selinux plug-in. (BZ#674717)

* The rhelVersion() function did not work correctly in Red Hat Enterprise Linux 5 and not all plug-ins consistently used the interface. This problem impacted a number of sos plug-ins (cluster, general, s390, and yum). With this update, the function now always returns the correct value and all the aforementioned plug-ins have been converted to use it. (BZ#710567)

In addition, this updated package provides the following enhancements:

* Prior to this update, the user could not change the target location for storing sos reports. Due to this, sos reports were not collected if the /tmp/ directory was full. This update adds the "--tmp-dir" option to the sosreport utility to allow the user to specify the target directory. (BZ#562283)

* Prior to this update, the user sometimes had to run several tools to diagnose issues on high-availability clusters. This update adds several enhancements to the cluster plug-in to provide more detailed information. (BZ#584060)

* Prior to this update, sosreport excluded files larger than 15 MB. With this update, such files are truncated to 15 MB so as to include the latest events and saved in the /sosreport/sos_commands/ directory. (BZ#636472)

* With this update, sos supports next-generation X.509 entitlement certificates. These certificates are captured and included in sos reports. (BZ#678666)

* With this update, sos reports include the content of the /etc/rhsm/ directory. (BZ#714296)

All users are advised to upgrade to this updated sos package, which fixes these bugs and adds these enhancements.

1.159. SPACEWALK-JAVA

1.159.1. RHSA-2011:0879: Moderate Red Hat Network Satellite server spacewalk-java security update

Updated spacewalk-java packages that fix one security issue are now available for Red Hat Network Satellite 5.4.1 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.

Red Hat Network (RHN) Satellite provides a solution to organizations requiring absolute control over and privacy of the maintenance and package deployment of their servers. It allows organizations to utilize the benefits of the Red Hat Network without having to provide public Internet access to their servers or other client systems.

It was found that RHN Satellite did not protect against Cross-Site Request Forgery (CSRF) attacks. If an authenticated RHN Satellite user visited a specially-crafted web page, it could lead to unauthorized command execution with the privileges of that user, for example, creating a new user account, granting administrator privileges to user accounts, disabling the account of the current user, and so on. (CVE-2009-4139)

Red Hat would like to thank Christian Johansson of Bitsec AB and Thomas Biege of the SUSE Security Team for independently reporting this issue.

Users of Red Hat Network Satellite 5.4.1 are advised to upgrade to these updated spacewalk-java packages, which resolve this issue. For this update to take effect, Red Hat Network Satellite must be restarted. Refer to the Solution section for details.

1.160. SPAMASSASSIN

1.160.1. RHBA-2011:1035: spamassassin bug fix and enhancement update

An updated spamassassin package that fixes various bugs and adds an enhancement is now available for Red Hat Enterprise Linux 5.

SpamAssassin provides a way to filter unsolicited email (spam messages) from incoming email.

The spamassassin package has been upgraded to the upstream version 3.3.1, which includes the default upstream rules and provides a number of bug fixes over the previous version. In order to keep the rules up-to-date, it is strongly recommended to allow the nightly rules update. This can be done by removing the comment sign from the following line in the /etc/cron.d/sa-update file:

#10 4 * * * root /usr/share/spamassassin/sa-update.cron 2>&1 | tee -a /var/log/sa-update.log

The regular update of the upstream rules ensures the SpamAssassin's best functionality. (BZ#481616)

In addition, this updated package fixes the following bug:

* Due to an incorrect "FH_DATE_PAST_20XX" filter rule, many emails containing the date 2010 in the message header were wrongly regarded as spam. According to the rule, all email messages containing the date between 2010 and 2099 had the spam score increased. To fix this problem, the rule "FH_DATE_PAST_20XX" has been modified to reflect the current year. (BZ#552127)

All users of spamassassin are advised to upgrade to this updated package, which resolves this issue and adds this enhancement.

1.161. SPICE-XPI

1.161.1. RHSA-2011:0427: Moderate spice-xpi security update

An updated spice-xpi package that fixes one security issue is 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.

The Simple Protocol for Independent Computing Environments (SPICE) is a remote display protocol used in Red Hat Enterprise Linux for viewing virtualized guests running on the Kernel-based Virtual Machine (KVM) hypervisor, or on Red Hat Enterprise Virtualization Hypervisor.

The spice-xpi package provides a plug-in that allows the SPICE client to run from within Mozilla Firefox.

An uninitialized pointer use flaw was found in the SPICE Firefox plug-in. If a user were tricked into visiting a malicious web page with Firefox while the SPICE plug-in was enabled, it could cause Firefox to crash or, possibly, execute arbitrary code with the privileges of the user running Firefox. (CVE-2011-1179)

Users of spice-xpi should upgrade to this updated package, which contains a backported patch to correct this issue. After installing the update, Firefox must be restarted for the changes to take effect.

1.162. SSSD

1.162.1. RHSA-2011:0975: Low sssd security, bug fix, and enhancement update

Updated sssd packages that fix one security issue, several bugs, and add various enhancements 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 linked to from the security description below.

The System Security Services Daemon (SSSD) provides a set of daemons to manage access to remote directories and authentication mechanisms. It provides an NSS and PAM interface toward the system and a pluggable back-end system to connect to multiple different account sources. It is also the basis to provide client auditing and policy services for projects such as FreeIPA.

IMPORTANT

This update was released as errata RHSA-2011:0975 – Low: sssd security, bug fix, and enhancement update.

Security fix:
A flaw was found in the `SSSD PAM responder` that could allow a local attacker to force SSSD to enter an infinite loop via a carefully-crafted packet. With SSSD unresponsive, legitimate users could be denied the ability to log in to the system. (CVE-2010-4341)

Red Hat would like to thank *Sebastian Krahmer* for reporting this issue.

Bug Fixes:

BZ#675007

While running the **LDAP cache cleanup** task, an issue with a corrupted **group cache** occurred, and the user was stripped of membership of every group except his primary group. This issue has been fixed and the aforementioned problem now no longer occurs.

BZ#676027

When the LDAP server defined in the first **ldap_uri** entry was unreachable, the login attempt to the system failed with a segmentation fault due to an issue in the failover processing. With this update, the segmentation fault no longer occurs if the first LDAP server can't be reached.

BZ#678412

Modifying or deleting a user or group account on an LDAP server did not result in an update of the cache on a login attempt. With this update, the cache is always properly updated during the login process. Outside of a login attempt, entries now remain as they were cached until the cache timeout expires.

BZ#678778

When performing an **initgroups()** request on a user, the IPA provider did not properly remove group memberships from the local cache when they were removed from the IPA server. With this update, a removed group is no longer present in the local cache.

BZ#691900

Previously, when **GECOS** information (an entry in the **/etc/passwd** file) for a user was missing, SSSD did not look for this information in the **cn** attribute as it should have. SSSD now correctly falls back to the **cn** attribute for **GECOS** if the GECOS field is empty, making SSSD fully compliant with section 5.3 of *RFC 2307*.

BZ#694149

For large cache files, if a user was removed from a group in LDAP, memory allocation could grow exponentially while processing the removal from the cache, potentially resulting in an OOM (Out of Memory) situation. With this update, this issue has been fixed, and SSSD no longer allocates unnecessarily large amounts of memory when removing a user from a group in LDAP.

BZ#707574

When the first DNS entry defined in the **/etc/resolv.conf** file was unreachable, SSSD failed to connect to any subsequent DNS server to resolve the **SRV record**. This caused SSSD to permanently operate in offline mode. This bug has been fixed and SSSD is now able to connect to an alternate server if the primary server is down.

BZ#665314

The following bugs have also been fixed:

- Issues with **LDAP search filters** that require escaping.
- Nested group issues with **RFC2307bis LDAP** servers without the **memberOf** plug-in.
- Several thread-safety issues in the **sss_client** code.

Enhancements:

BZ#665314

The sssd package has been upgraded to upstream version 1.5.1, which provides a number of bug fixes and enhancements over the previous version. The following enhancements are the most significant:

- Support for delayed online **Kerberos** authentication has been improved.
- A Kerberos access provider to honor the **.k5login** authorization file has been added.
- The verbosity of **PAM_TEXT_INFO** messages for cached credentials has been reduced.
- Group support to the **simple access provider** has been added.
- The time delay between connecting to a network or VPN and acquiring a TGT (Ticket Granting Ticket) has been significantly reduced.
- A feature for the automatic Kerberos ticket renewal has been added.
- SSSD now provides a Kerberos ticket for long-lived processes or cron jobs even when the user logs out.
- Several new features to the **LDAP access provider** have been added.
- Support for **shadow** access control has been added.
- Support for the **authorizedService** access control has been added.
- The ability to mix-and-match **LDAP** access control features has been added.
- An option for a separate password-change LDAP server for platforms not supporting LDAP referrals has been added.
- Support for manual page translations has been added.
- Support for searching out and returning information about netgroups stored in LDAP has been added.
- The performance of group processing of **RFC2307 LDAP** servers has been improved.
- A new option, **dns_discovery_domain**, which allows for better configuration of **SRV records** for failover, has been added.

Users of **SSSD** should upgrade to these updated packages, which upgrade sssd to upstream version 1.5.1 to correct this issue, fix these bugs, and add these enhancements.

1.163. SUBVERSION

1.163.1. RHSA-2011:0862: Moderate subversion security update

Updated subversion packages that fix three security issues are now available for Red Hat Enterprise Linux 5 and 6.

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.

Subversion (SVN) is a concurrent version control system which enables one or more users to collaborate in developing and maintaining a hierarchy of files and directories while keeping a history of all changes. The mod_dav_svn module is used with the Apache HTTP Server to allow access to Subversion repositories via HTTP.

An infinite loop flaw was found in the way the mod_dav_svn module processed certain data sets. If the SVNPathAuthz directive was set to "short_circuit", and path-based access control for files and directories was enabled, a malicious, remote user could use this flaw to cause the httpd process serving the request to consume an excessive amount of system memory. (CVE-2011-1783)

A NULL pointer dereference flaw was found in the way the mod_dav_svn module processed requests submitted against the URL of a baselined resource. A malicious, remote user could use this flaw to cause the httpd process serving the request to crash. (CVE-2011-1752)

An information disclosure flaw was found in the way the mod_dav_svn module processed certain URLs when path-based access control for files and directories was enabled. A malicious, remote user could possibly use this flaw to access certain files in a repository that would otherwise not be accessible to them. Note: This vulnerability cannot be triggered if the SVNPathAuthz directive is set to "short_circuit". (CVE-2011-1921)

Red Hat would like to thank the Apache Subversion project for reporting these issues. Upstream acknowledges Joe Schaefer of the Apache Software Foundation as the original reporter of CVE-2011-1752; Ivan Zhakov of VisualSVN as the original reporter of CVE-2011-1783; and Kamesh Jayachandran of CollabNet, Inc. as the original reporter of CVE-2011-1921.

All Subversion users should upgrade to these updated packages, which contain backported patches to correct these issues. After installing the updated packages, you must restart the httpd daemon, if you are using mod_dav_svn, for the update to take effect.

1.163.2. RHSA-2011:0327: Moderate subversion security and bug fix update

Updated subversion packages that fix one security issue and one bug 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.

Subversion (SVN) is a concurrent version control system which enables one or more users to collaborate in developing and maintaining a hierarchy of files and directories while keeping a history of all changes. The mod_dav_svn module is used with the Apache HTTP Server to allow access to Subversion repositories via HTTP.

A NULL pointer dereference flaw was found in the way the mod_dav_svn module processed certain requests to lock working copy paths in a repository. A remote attacker could issue a lock request that could cause the httpd process serving the request to crash. (CVE-2011-0715)

Red Hat would like to thank Hyrum Wright of the Apache Subversion project for reporting this issue. Upstream acknowledges Philip Martin, WANdisco, Inc. as the original reporter.

This update also fixes the following bug:

* A regression was found in the handling of repositories which do not have a "db/fsfs.conf" file. The

"svnadmin hotcopy" command would fail when trying to produce a copy of such a repository. This command has been fixed to ignore the absence of the "fsfs.conf" file. The "svnadmin hotcopy" command will now succeed for this type of repository. (BZ#681522)

All Subversion users should upgrade to these updated packages, which contain backported patches to correct these issues. After installing the updated packages, you must restart the httpd daemon, if you are using mod_dav_svn, for the update to take effect.

1.163.3. RHSA-2011:0257: Moderate subversion security update

Updated subversion packages that fix two security issues 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.

Subversion (SVN) is a concurrent version control system which enables one or more users to collaborate in developing and maintaining a hierarchy of files and directories while keeping a history of all changes.

A server-side memory leak was found in the Subversion server. If a malicious, remote user performed "svn blame" or "svn log" operations on certain repository files, it could cause the Subversion server to consume a large amount of system memory. (CVE-2010-4644)

A NULL pointer dereference flaw was found in the way the mod_dav_svn module (for use with the Apache HTTP Server) processed certain requests. If a malicious, remote user issued a certain type of request to display a collection of Subversion repositories on a host that has the SVNListParentPath directive enabled, it could cause the httpd process serving the request to crash. Note that SVNListParentPath is not enabled by default. (CVE-2010-4539)

All Subversion users should upgrade to these updated packages, which contain backported patches to correct these issues. After installing the updated packages, the Subversion server must be restarted for the update to take effect: restart httpd if you are using mod_dav_svn, or restart svnserve if it is used.

1.164. SYSFSUTILS

1.164.1. RHEA-2011:1047: sysfsutils enhancement update

Updated sysfsutils packages that add one enhancement are now available for Red Hat Enterprise Linux 5.

The sysfsutils utility provides a set of daemons to manage access to remote directories and authentication mechanisms. It provides an NSS and PAM interface toward the system and a pluggable backend system to connect to multiple different account sources. It is also the basis to provide client auditing and policy services for projects like FreeIPA.

The sysfsutils packages have been upgraded to version 2.1.0, which adds several previously missing application programming interface (API) functions. (BZ#605292)

All sysfsutils users are advised to upgrade to these updated sysfsutils packages, which add this enhancement.

1.165. SYSSTAT

1.165.1. RHSA-2011:1005: Low sysstat security, bug fix, and enhancement update

An updated sysstat package that fixes one security issue, various bugs, and adds one enhancement is 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 sysstat package contains a set of utilities which enable system monitoring of disks, network, and other I/O activity.

It was found that the sysstat initscript created a temporary file in an insecure way. A local attacker could use this flaw to create arbitrary files via a symbolic link attack. (CVE-2007-3852)

This update fixes the following bugs:

* On systems under heavy load, the sadc utility would sometimes output the following error message if a write() call was unable to write all of the requested input:

"Cannot write data to system activity file: Success."

In this updated package, the sadc utility tries to write the remaining input, resolving this issue. (BZ#454617)

* On the Itanium architecture, the "sar -I" command provided incorrect information about the interrupt statistics of the system. With this update, the "sar -I" command has been disabled for this architecture, preventing this bug. (BZ#468340)

* Previously, the "iostat -n" command used invalid data to create statistics for read and write operations. With this update, the data source for these statistics has been fixed, and the iostat utility now returns correct information. (BZ#484439)

* The "sar -d" command used to output invalid data about block devices. With this update, the sar utility recognizes disk registration and disk overflow statistics properly, and only correct and relevant data is now displayed. (BZ#517490)

* Previously, the sar utility set the maximum number of days to be logged in one month too high. Consequently, data from a month was appended to data from the preceding month. With this update, the maximum number of days has been set to 25, and data from a month now correctly replaces data from the preceding month. (BZ#578929)

* In previous versions of the iostat utility, the number of NFS mount points was hard-coded. Consequently, various issues occurred while iostat was running and NFS mount points were mounted or unmounted; certain values in iostat reports overflowed and some mount points were not reported at all. With this update, iostat properly recognizes when an NFS mount point mounts or unmounts, fixing these issues. (BZ#675058, BZ#706095, BZ#694767)

* When a device name was longer than 13 characters, the iostat utility printed a redundant new line character, making its output less readable. This bug has been fixed and now, no extra characters are printed if a long device name occurs in iostat output. (BZ#604637)

* Previously, if kernel interrupt counters overflowed, the sar utility provided confusing output. This bug has been fixed and the sum of interrupts is now reported correctly. (BZ#622557)

* When some processors were disabled on a multi-processor system, the sar utility sometimes failed to provide information about the CPU activity. With this update, the uptime of a single processor is used to compute the statistics, rather than the total uptime of all processors, and this bug no longer occurs. (BZ#630559)

* Previously, the mpstat utility wrongly interpreted data about processors in the system. Consequently, it reported a processor that did not exist. This bug has been fixed and non-existent CPUs are no longer reported by mpstat. (BZ#579409)

* Previously, there was no easy way to enable the collection of statistics about disks and interrupts. Now, the SADC_OPTIONS variable can be used to set parameters for the sadc utility, fixing this bug. (BZ#598794)

* The read_uptime() function failed to close its open file upon exit. A patch has been provided to fix this bug. (BZ#696672)

This update also adds the following enhancement:

* With this update, the cifsiostat utility has been added to the sysstat package to provide CIFS (Common Internet File System) mount point I/O statistics. (BZ#591530)

All sysstat users are advised to upgrade to this updated package, which contains backported patches to correct these issues and add this enhancement.

1.166. SYSTEM-CONFIG-CLUSTER

1.166.1. RHBA-2011:1066: system-config-cluster bug fix and enhancement update

An updated system-config-cluster package that fixes a bug and provides an enhancement is now available for Red Hat Enterprise Linux 5.

The system-config-cluster package contains a utility that allows the management of cluster configuration in a graphical setting.

This updated system-config-cluster package fixes the following bug:

* When the fence_ipmilan fence device agent attribute was used with the lanplus option, the validation of the cluster.conf file against the cluster.ng schema produced unexpected errors. This issue has been resolved by defining the "ipaddr" attribute in fence attribute group definitions as optional. (BZ#642521)

In addition, this updated package provides the following enhancement:

* Documentation for the cluster.conf schema is now provided. (BZ#645816)

All users are advised to upgrade to this updated system-config-cluster package, which resolves this issue and adds this enhancement.

1.167. SYSTEM-CONFIG-KICKSTART

1.167.1. RHBA-2011:1025: system-config-kickstart bug fix update

An updated system-config-kickstart package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The system-config-kickstart package contains the Kickstart Configurator, a graphical tool for creating kickstart files.

This updated package fixes the following bug:

* Prior to this update,system-config-kickstart did not handle IOError (Input/output error) exceptions when trying to read the file given on the command line. Due to this behavior, system-config-kickstart terminated unexpectedly when it was started from the command line with a non-existing file. This update allows IOError exceptions. Now, an error dialog is displayed if an IOError occurs. (BZ#431950)

All system-config-kickstart users are advised to upgrade to this updated package, which fixes this bug.

1.168. SYSTEM-CONFIG-LVM

1.168.1. RHBA-2011:1036: system-config-lvm bug fix update

An updated system-config-lvm package that fixes two bugs is now available for Red Hat Enterprise Linux 5.

The system-config-lvm package contains a graphical application for the configuration of LVM logical volumes.

This updated system-config-lvm package includes fixes for the following bugs:

* A logical volume could have been specified as not being mounted in the system-config-lvm GUI even though it actually was mounted, which prevented the possibility of performing certain operations, such as volume resizing. This update corrects this error so that the mount state of a volume is correctly represented, and operations on the volume can be carried out as expected. (BZ#672475)

* During the process of creating a new logical volume and ensuring that it persists across reboots, the system-config-lvm application could have become unresponsive and failed to create the appropriate /etc/fstab entry. This update corrects this error so that the application no longer potentially hangs during the process, and the /etc/fstab entry is successfully written. (BZ#672948)

All users of system-config-lvm are advised to upgrade to this updated package, which resolves these issues.

1.168.2. RHBA-2011:0898: system-config-lvm bug fix update

An updated system-config-lvm package that fix 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:

* Recent updates to the GNU core utilities (coreutils) package included a move of the readlink command from /usr/bin/readlink to /bin/readlink. The Logical Volume Management utility was updated to reflect this move. On Red Hat Enterprise Linux 5, however, readlink is still installed to /usr/bin/readlink. As a consequence, system-config-lvm erroneously presented mounted logical volumes as Not Mounted and, equally erroneously, reported their "Mount Point when Rebooted" as "None". As well, when trying to resize such a volume, the utility presented the following (also erroneous) message:

Logical volume is not mounted but is in use. Please close all applications using this device.

With this update, system-config-lvm running on Red Hat Enterprise Linux 5 once again looks for readlink at /usr/bin/readlink and, consequently, reports the properties of mounted volumes correctly and allows re-sizing of such volumes as expected. (BZ#579049)

All system-config-lvm users should upgrade to this updated package, which resolves this issue.

1.169. SYSTEM-CONFIG-NETBOOT

1.169.1. RHBA-2011:0829: system-config-netboot bug fix update

Updated system-config-netboot packages that resolve several issues are now available for Red Hat Enterprise Linux 5.

System-config-netboot is a utility which allows you to configure diskless environments and network installations.

These updated system-config-netboot packages provide fixes for the following bugs:

* Installation scripts erroneously overwrote ".msg" files under the /tftpboot/linux-install/msgs/ directory, regardless of whether they were modified, when installing the system-config-netboot utility. Certain of these ".msg" configuration files were important for the system build process. With this update, the ".msg" files in that directory are now treated as configuration files, and are therefore not overwritten if they have been modified. (BZ#459383)

* Certain programs such as nscd, the name service caching daemon, required the /var/db/ directory to be writable in order to function correctly. This update adds the /var/db/ directory to the snapshot so that it is writeable, with the result that services which depend on a writable /var/db/ directory, such as LDAP, now function as expected. (BZ#504179)

* The sequence of steps to perform in order to set up automounting are included in the documentation provided in the system-config-netboot packages. Following these instructions did not succeed as expected because of the omission of a step instructing users to create a symbolic link from the /proc/mounts file to the /etc/mtab file. This update adds this step to the documentation, and the automount setup instructions are now complete. (BZ#504231)

* Incorrect text in a network connection error dialog was displayed when performing a "Network Install". This was caused by a Unicode encoding issue that has been fixed in this update, with the result that the error message displayed under the same circumstances is now correct. (BZ#579666)

All users of system-config-netboot are advised to upgrade to these updated packages, which resolve these issues.

1.170. SYSTEM-CONFIG-NETWORK

1.170.1. RHBA-2011:0817: system-config-network bug fix update

Updated system-config-network packages that fix a bug are now available for Red Hat Enterprise Linux 5.

The system-config-network packages provide network configuration utilities for both the graphical user interface and command line. These utilities support Ethernet, wireless, IPsec, Token Ring, ADSL, ISDN, and PPP.

This update fixes the following bug:

* When the /etc/hosts configuration file contained an invalid entry (for example, an IP address without a hostname), an attempt to run the system-config-network utility failed with a traceback written to standard error. This update corrects the utility to verify that the /etc/hosts file does not contain erroneous lines. As a result, when an invalid entry is present, a warning message is displayed, and system-config-network starts as expected. (BZ#492915)

All users of system-config-network are advised to upgrade to these updated packages, which resolve this issue.

1.171. SYSTEMTAP

1.171.1. RHSA-2011:0841: Moderate systemtap security update

Updated systemtap 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 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.

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 divide-by-zero flaw was found in the way SystemTap handled malformed debugging information in DWARF format. When SystemTap unprivileged mode was enabled, an unprivileged user in the stapusr group could use this flaw to crash the system. Additionally, a privileged user (root, or a member of the stapdev group) could trigger this flaw when tricked into instrumenting a specially-crafted ELF binary, even when unprivileged mode was not enabled. (CVE-2011-1769)

SystemTap users should upgrade to these updated packages, which contain a backported patch to correct this issue.

1.171.2. RHBA-2011:1044: systemtap bug fix update

Updated systemtap packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

SystemTap is an instrumentation system for systems running the Linux kernel. The system allows developers to write scripts to collect data on the operation of the system.

This update fixes the following bugs:

* Previously, the buildok/fortyfive.stp test case failed to build with SystemTap on the Itanium systems. The problem has been fixed in this update. (BZ#559599)

* Previously, the systemtap service was not stopped and restarted after the "service systemtap stop" and "service systemtap restart" commands were issued. Instead, the service only stopped and was not restarted. This update fixes the problem so that the systemtap service now behaves as expected. (BZ#607232)

* Previously, there was a timing issue when running the "service systemtap restart" command in that a test case for the systemtap-initscript package sometimes failed to restart the service when a script was running. This issue has been resolved with this update so that the command runs correctly now. (BZ#644350)

* After prelink had been run on a system based on the i686 platform, using SystemTap user-space

probes that targeted functions or statements in certain shared libraries, or executables based on a separate debuginfo file, caused resolution to the wrong PC location in a linked binary. As a result, the intended probes failed to fire at the correct place in the program, which could have caused the program to crash or misbehave due to a corrupted instruction sequence resulting from incorrect breakpoint insertions. With this update, the libdwfl library code (the libdw.so shared object library) was adjusted to use a more reliable method of compensating for prelink's effect on the address layout of a binary when aligning a runtime PC address with an address computed separately from the separated debuginfo file. SystemTap probes should now work the same on prelinked binaries as they would on binaries that have not been prelinked. (BZ#646870)

* On the i386 platform, there was a semantic error found in the buildok/scheduler-ctxswitch.stp test case, which limited SystemTap's testsuite and tapset portability. This update fixes the problem. (BZ#661424)

* Previously, an itrace (process("PROC").insn) probe could have resulted in a kernel panic as a result of an incorrect PID being used when setting up the probe. The problem has been fixed in this update so that the probe no longer results in a kernel panic. (BZ#699342)

All users requiring SystemTap are advised to upgrade to these updates packages, which fix these bugs.

1.172. SYSVINIT

1.172.1. RHBA-2011:1040: SysVinit bug fix update

An updated SysVinit package that fixes several bugs is now available for Red Hat Enterprise Linux 5.

The SysVinit package contains a group of processes that control the basic functions of your system. SysVinit includes the init program, which is the first program started by the Linux kernel when the system boots. The init program then controls the starting up and shutting down of all other programs.

This update fixes the following bugs:

* Prior to this update, the command "pidof" did not return a process identifier (PID) if run as the root user and the path name began with "/". The problem is resolved in this update so that "pidof" now returns the PID as expected. (BZ#507382, BZ#589668)

* Prior to this update, the command "pidof" unexpectedly issued an error message under certain circumstances. The error message was similar to "can't get program name from /proc/[pid]/stat", or "can't read sid from /proc/[pid]/stat". This unintended behavior is corrected with this update and no longer occurs. (BZ#592956)

* Prior to this update, using the command "last" to view current and previous logins displayed a truncated username if the username was over 8 characters long. With this update, the option "-w" / "--wide" has been added to the "last" command to support wide output. (BZ#673533)

* Prior to this update, non-privileged users could have received incorrect service status information when running the command "service [service] status". The problem is fixed in this update so that after running the command, the service status information is correctly displayed along with an error message indicating that the command was run by a non-privileged user. (BZ#684881)

* Prior to this update, when a user logged in from an IPv6 host and the command "last" was used to display the IP address, the command "last" displayed an incorrect IPv4 format address, which only included the first 32 bits of the actual IPv6 address. The problem is fixed so that the command "last" now displays the correct IPv6 format address. (BZ#690939)

Users are advised to upgrade to this updated SysVinit package, which fixes these bugs.

1.173. TALK

1.173.1. RHEA-2011:0828: talk enhancement update

Updated talk packages that add one enhancement are now available for Red Hat Enterprise Linux 5.

The talk utility is a communication program that copies lines from one terminal to the terminal of another user.

This update adds the following enhancement:

* The talk utility allows a user to specify the target user in the "username.hostname" form. Consequent to this, previous versions of the utility did not support usernames that contained a period. With this update, a new command line option (that is, "-x") has been added to enforce the use of the "username@hostname" form, so that the username can contain periods. As well, the corresponding manual page has been extended to provide a complete list of supported command line arguments. (BZ#574451)

All users of talk are advised to upgrade to these updated packages, which add this enhancement.

1.174. TETEX

1.174.1. RHBA-2011:0458: tetex bug fix update

Updated tetex packages that resolve a bug are now available for Red Hat Enterprise Linux 5.

teTeX is an implementation of TeX. TeX takes a text file and a set of formatting commands as input, and creates a typesetter-independent DeVice Independent (DVI) file.

These updated tetex packages fix the following bug:

* Previously, an error could have occurred and was logged when installing teTeX. This happened because several files installed in the /usr/share/texmf/ directory used an incorrect SELinux context. With this update, the files use the correct SELinux context and installation finishes without errors. (BZ#448099)

All users of teTeX are advised to upgrade to these updated packages, which fix this bug.

1.175. THUNDERBIRD

1.175.1. RHSA-2011:0887: Critical thunderbird security update

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

The Red Hat Security Response Team has rated this update as having critical 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.

Mozilla Thunderbird is a standalone mail and newsgroup client.

A flaw was found in the way Thunderbird handled malformed JPEG images. An HTML mail message containing a malicious JPEG image could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird. (CVE-2011-2377)

Multiple dangling pointer flaws were found in Thunderbird. Malicious HTML content could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird. (CVE-2011-0083, CVE-2011-0085, CVE-2011-2363)

Several flaws were found in the processing of malformed HTML content. Malicious HTML content could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird. (CVE-2011-2364, CVE-2011-2365, CVE-2011-2374, CVE-2011-2375, CVE-2011-2376)

An integer overflow flaw was found in the way Thunderbird handled JavaScript Array objects. Malicious content could cause Thunderbird to execute JavaScript with the privileges of the user running Thunderbird. (CVE-2011-2371)

A use-after-free flaw was found in the way Thunderbird handled malformed JavaScript. Malicious content could cause Thunderbird to execute JavaScript with the privileges of the user running Thunderbird. (CVE-2011-2373)

It was found that Thunderbird could treat two separate cookies (for web content) as interchangeable if both were for the same domain name but one of those domain names had a trailing "." character. This violates the same-origin policy and could possibly lead to data being leaked to the wrong domain. (CVE-2011-2362)

All Thunderbird users should upgrade to this updated package, which resolves these issues. All running instances of Thunderbird must be restarted for the update to take effect.

1.175.2. RHSA-2011:0474: Critical thunderbird security update

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

The Red Hat Security Response Team has rated this update as having critical 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.

Mozilla Thunderbird is a standalone mail and newsgroup client.

Several flaws were found in the processing of malformed HTML content. An HTML mail message containing malicious content could possibly lead to arbitrary code execution with the privileges of the user running Thunderbird. (CVE-2011-0080)

An arbitrary memory write flaw was found in the way Thunderbird handled out-of-memory conditions. If all memory was consumed when a user viewed a malicious HTML mail message, it could possibly lead to arbitrary code execution with the privileges of the user running Thunderbird. (CVE-2011-0078)

An integer overflow flaw was found in the way Thunderbird handled the HTML frameset tag. An HTML mail message with a frameset tag containing large values for the "rows" and "cols" attributes could trigger this flaw, possibly leading to arbitrary code execution with the privileges of the user running Thunderbird. (CVE-2011-0077)

A flaw was found in the way Thunderbird handled the HTML iframe tag. An HTML mail message with an iframe tag containing a specially-crafted source address could trigger this flaw, possibly leading to arbitrary code execution with the privileges of the user running Thunderbird. (CVE-2011-0075)

A flaw was found in the way Thunderbird displayed multiple marquee elements. A malformed HTML mail message could cause Thunderbird to execute arbitrary code with the privileges of the user running Thunderbird. (CVE-2011-0074)

A flaw was found in the way Thunderbird handled the nsTreeSelection element. Malformed content could cause Thunderbird to execute arbitrary code with the privileges of the user running Thunderbird. (CVE-2011-0073)

All Thunderbird users should upgrade to this updated package, which resolves these issues. All running instances of Thunderbird must be restarted for the update to take effect.

1.175.3. RHSA-2011:0374: Important thunderbird security and bug fix update

An updated thunderbird package that fixes one security issue and one bug is now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having important security impact.

Mozilla Thunderbird is a standalone mail and newsgroup client.

This erratum blacklists a small number of HTTPS certificates. (BZ#689430)

This update also fixes the following bug:

* The RHSA-2011:0312 and RHSA-2011:0311 updates introduced a regression, preventing some Java content and plug-ins written in Java from loading. With this update, the Java content and plug-ins work as expected. (BZ#683076)

All Thunderbird users should upgrade to this updated package, which resolves these issues. All running instances of Thunderbird must be restarted for the update to take effect.

1.175.4. RHSA-2011:0312: Moderate thunderbird security update

An updated thunderbird package that fixes several security issues is now available for Red Hat Enterprise Linux 4 and 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.

Mozilla Thunderbird is a standalone mail and newsgroup client.

Several flaws were found in the processing of malformed HTML content. Malicious HTML content could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird. (CVE-2011-0051, CVE-2011-0053)

Note: JavaScript support is disabled by default in Thunderbird. The above issues are not exploitable unless JavaScript is enabled.

All Thunderbird users should upgrade to this updated package, which resolves these issues. All running instances of Thunderbird must be restarted for the update to take effect.

1.176. TOMCAT5

1.176.1. RHSA-2011:0336: Important tomcat5 security update

Updated tomcat5 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 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.

Apache Tomcat is a servlet container for the Java Servlet and JavaServer Pages (JSP) technologies.

A denial of service flaw was found in the way certain strings were converted to Double objects. A remote attacker could use this flaw to cause Tomcat to hang via a specially-crafted HTTP request. (CVE-2010-4476)

Users of Tomcat should upgrade to these updated packages, which contain a backported patch to correct this issue. Tomcat must be restarted for this update to take effect.

1.176.2. RHBA-2011:0954: tomcat5 bug fix update

Updated tomcat5 packages that resolve several issues are now available for Red Hat Enterprise Linux 5.

Apache Tomcat is a servlet container for the Java Servlet and JavaServer Pages (JSP) technologies.

These updated tomcat5 packages provide fixes for the following bugs:

* When the tomcat server parsed a cookie whose name contained either single- or double-quotes and then passed that cookie name and value to a servlet, any quotes were removed from the cookie name and the cookie had an empty value. This update corrects the parsing so that single- or double-quotes can be used inside cookie names without information loss. (BZ#717456)

* When any context.xml configuration file did not specify a Document Base directory (which is also called the Context Root), tomcat failed to start up due to the missing Document Base causing a NullPointerException. As a workaround, the Document Base could be defined in the context.xml file, and this would prevent the exception and allow the server to start. With this update, a missing Document Base in any context.xml file no longer causes a NullPointerException at server startup. (BZ#717457)

All users of tomcat5 are advised to upgrade to these updated packages, which resolve these issues.

1.177. TOTEM

1.177.1. RHBA-2011:0215: totem bug fix update

An updated totem package that fixes one bug is now available for Red Hat Enterprise Linux 5.

Totem is a simple movie player for the GNOME desktop. It features a simple playlist, a full-screen mode, seek and volume controls, as well as complete keyboard navigation.

This update fixes the following bug:

* Previously, video content on the website: http://www.apple.com/trailers/ did not work with totem. This update overrides the User-Agent HTTP headers. Now, users can play videos from this website without further error messages.

All users wishing to view trailers on this website are advised to upgrade to this updated package, which fixes this bug.

1.178. TRACEROUTE

1.178.1. RHBA-2011:0469: traceroute bug fix update

An updated traceroute package that fixes two bugs is now available for Red Hat Enterprise Linux 5.

The traceroute utility displays the route used by IP packets on their way to a specified network (or Internet) host. Traceroute displays the IP address and hostname (if possible) of the machines along the route taken by the packets.

This update fixes the following bugs:

* Prior to this update, using the "-m" command line option to specify the maximum time-to-live (TTL) value in the range 1 to 5 caused the traceroute utility to fail with the following error:

sim hops out of range

This update applies an upstream patch to ensure that all TTL values in the range from 1 to 255 are supported as expected. (BZ#461278)

* Previously, using the "-l" command line option to specify the flow label of the probing packets caused the utility to fail with the following error:

setsockopt IPV6_FLOWLABEL_MGR: Operation not permitted

With this update, the underlying source code has been modified to address this issue, and using the "-l" option no longer causes traceroute to fail. (BZ#644297)

All users of traceroute are advised to upgrade to this updated package, which fixes these bugs.

1.179. UDEV

1.179.1. RHBA-2011:1046: udev bug fix update

Updated udev packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

The udev packages implement a dynamic device-directory, providing only the devices present on the system. This dynamic directory runs in user space, dynamically creates and removes devices, provides consistent naming, and a user space API. udev replaces devfs, providing greater hot plug functionality.

This update fixes the following bugs:

* Previously, the udev helper application scsi_id left temporary devices nodes in the /dev directory. These devices nodes could have been captured by the "pvscan" command and shown in the "pvdisplay" device listing. This unintended behavior no longer occurs with this update. (BZ#677203)

* Previously, the udev daemon was killed and started if the udev package was installed in a chrooted environment. This update prevents restarting the daemon. (BZ#699711)

* Previously, the udev daemon created symbolic links to tape devices in the /dev/disk directory with a wrong name, and not for all tape devices present on the system. With this update, udev now correctly creates symbolic links for all tape devices in /dev/disk as expected. (BZ#689957)

Users are advised to upgrade to these updated udev packages, which fix these bugs.

1.180. VALGRIND

1.180.1. RHBA-2011:1026: valgrind bug fix update

An updated valgrind package that fixes various bugs is now available for Red Hat Enterprise Linux 5.

The valgrind tool helps to detect memory-management problems in programs.

This updated valgrind package includes fixes for the following bugs:

* When testing prelinked programs, valgrind could have crashed due to a segmentation fault due to a failed assertion. This was caused by the prelink utility handling the .bss section incorrectly. This update corrects this assertion so that it no longer fails in the described scenario. (BZ#587338)

* Previously, when compiling a file against the valgrind pub_tool_basics.h header using gcc, the compilation failed with this error message:

config.h: No such file or directory.

This was caused by the config.h file which was not a part of the valgrind package, but was required by the pub_tool_basics.h header. The macro from the config.h file used before was replaced by the __GNUC__ macro. This fixes the problem and the compilation runs clean. (BZ#649272)

All users of valgrind are advised to upgrade to this updated package, which resolves these bugs.

1.181. VIRT-MANAGER

1.181.1. RHBA-2011:1055: virt-manager bug fix update

An updated virt-manager package that fixes various bugs is now available for Red Hat Enterprise Linux 5.

Virtual Machine Manager (virt-manager) is a graphical tool for administering virtual machines for KVM, Xen and QEMU. The virt-manager utility 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. It uses the libvirt API (Application Programming Interface).

This updated virt-manager package includes fixes for the following bugs:

* When the media in a CD-ROM device has been changed in a KVM guest configuration, virt-manager specified the disk driver name incorrectly as "file" or "phy" instead of the correct name, "qemu". This caused the KVM domain that the guest was running in to fail to start. The issue has been fixed: virt-manager now assigns the disk driver name correctly and the domain is now successfully started after the resource change. (BZ#641858)

* When changing CPU allocation values for a KVM guest in the virtual hardware table using the virt-manager GUI, it was not possible to save new values. This happened because this operation was considered invalid for an inactive KVM domain. This issue has been fixed and the CPU allocation values change is now respected in the virt-manager GUI. (BZ#644736)

* Previously, an attempt to change the current memory allocation value for a KVM guest in the virtual hardware table using the virt-manager GUI failed with an error message saying that this function is not supported by a connection driver. This problem has been fixed and a user is now able to change the current memory allocation value by using the virt-manager GUI. (BZ#645285)

All users of virt-manager are advised to upgrade to this updated package, which resolves these issues.

1.182. VIRTIO-WIN

1.182.1. RHBA-2011:0280: virtio-win bug fix update

An updated virtio-win package that fixes a bug is now available for Red Hat Enterprise Linux 5.

Para-virtualized drivers are virtualization-aware drivers used by fully-virtualized guests running on Red Hat Enterprise Linux. Fully-virtualized guests using the para-virtualized drivers gain significantly better I/O performance than fully-virtualized guests running without the drivers.

The virtio-win package provides para-virtualized network drivers for the following guest operating systems:

32-bit Windows XP 32-bit Windows Server 2003 64-bit Windows Server 2008 32-bit Windows Server 2008 64-bit Windows Server 2008 R2 32-bit Windows 7

The virtio-win package also provides para-virtualized disk (block) drivers for the following guest operating systems:

32-bit Windows XP 32-bit Windows Server 2003 64-bit Windows Server 2008 32-bit Windows Server 2008 64-bit Windows Server 2008 R2 32-bit Windows 7

This update fixes the following bug:

* Under certain circumstances, when a user installed a Windows guest on a Red Hat Enterprise Linux 5 host and then copied the image, an attempt to boot this image from virtio block device on a Red Hat Enterprise Linux 6 host could fail with an error screen. This error has been fixed, and such images now boot as expected on both Red Hat Enterprise Linux 5 and 6. (BZ#634529)

All users running fully-virtualized instances of Windows on Red Hat Enterprise Linux-based KVM hosts are advised to upgrade to this updated package, which resolves this issue.

1.183. VNC

1.183.1. RHBA-2011:0216: vnc bug fix update

Updated vnc packages that fix two bugs are now available for Red Hat Enterprise Linux 5.

Virtual Network Computing (VNC) is a remote display system 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.

This update fixes the following bugs:

* Prior to this update, the Xvnc server could refuse a connection when it received the SIGALRM signal during the reading of a password file. With this update, the underlying source code has been modified to address this issue, and receiving the SIGALRM signal no longer prevents clients from establishing a connection. (BZ#670249)

* On a system with more than 256 network interfaces, Xvnc terminated unexpectedly during startup. This error has been fixed, and Xvnc no longer crashes on systems with a large number of network interfaces. (BZ#673976)

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

1.184. VSFTPD

1.184.1. RHSA-2011:0337: Important vsftpd security update

An updated vsftpd package that fixes one security issue is now available for Red Hat Enterprise Linux 4, 5, and 6.

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.

vsftpd (Very Secure File Transfer Protocol (FTP) daemon) is a secure FTP server for Linux, UNIX, and similar operating systems.

A flaw was discovered in the way vsftpd processed file name patterns. An FTP user could use this flaw to cause the vsftpd process to use an excessive amount of CPU time, when processing a request with a specially-crafted file name pattern. (CVE-2011-0762)

All vsftpd users should upgrade to this updated package, which contains a backported patch to correct this issue. The vsftpd daemon must be restarted for this update to take effect.

1.184.2. RHBA-2011:0830: vsftpd bug fix update

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

The vsftpd package includes a Very Secure FTP (File Transfer Protocol) daemon.

This updated vsftpd package includes fixes for the following bugs:

* The previous version of vsftpd did not interpret wildcards correctly. As a result, applications relying on the wildcard functionality did not function properly. With this update, supported wildcards ('*' and '?') work as expected. (BZ#517292)

* When specific options were set in the configuration file, vsftpd prematurely closed the connection. This was caused by a child process which was responsible for handling post-auth commands and a patch which influenced the behavior of that child process. With this update, a termination signal is sent to the child process when its parent dies with the result that connections no longer prematurely close. (BZ#530706)

* Under certain circumstances, some clients could hang or behave slow due to a faulty double call to SSL_shutdown() in the ssl_data_close() function. With this update, the call has been fixed and a client no longer hangs or performs slowly. (BZ#556795)

* Prior to this update, vsftpd used the SIGUSR1 signal for signaling between child and parent processes. However, sending the SIGUSR1 signal could cause other applications to misbehave. With this update, the SIGUSR1 signal is only sent when the following parameter is set in the /etc/vsftpd.conf configuration file: "background=YES". (BZ#579317)

* Attempting to authenticate with an empty username and an empty password against a vsftpd server with Kerberos authentication failed and returned the following message: "500 OOPS: zero or big size in vsf_sysutil_malloc". With this update, vsftpd properly handles an attempt to authenticate with empty credentials. (BZ#619731)

* Prior to this update, when using the "use_localtime=YES" option, vsftpd did not take the DST specification into account. This caused the mtime value to be incorrectly interpreted for files that were last modified before the latest DST occurred. With this update, the DST is accounted for. (BZ#676254)

* Virtual guest accounts could be incorrectly logged as anonymous accounts in the xferlog file even if the use of anonymous accounts was disabled. With this update, a virtual guest account is properly logged. (BZ#680823)

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

1.185. W3M

1.185.1. RHBA-2011:0400: w3m bug fix update

Updated w3m packages that fix two bugs are now available for Red Hat Enterprise Linux 5.

The w3m program is a pager (or text file viewer) that can also be used as a text mode web browser.

This update fixes the following bugs:

* Prior to this update, the RPM spec file did not mark the /etc/w3m/config file "noreplace", allowing the update process to overwrite the configuration without a backup. This error has been fixed, and the /etc/w3m/config file with local changes is now properly backed up when the w3m package is updated. (BZ#615859)

* Previously, the NOTES section in the manual page for w3m incorrectly stated that the document is written for the 0.2.1 release of the program. This update corrects this information, and 0.5.1 is now used as expected. (BZ#615865)

All users of w3m are advised to upgrade to these updated packages, which resolve these issues.

1.186. WDAEMON

1.186.1. RHEA-2011:1062: wdaemon enhancement update

An updated wdaemon package that adds one enhancement is now available for Red Hat Enterprise Linux 5.

wdaemon is a helper application that emulates persistent input devices for Wacom tablets. This allows such devices to be plugged in and unplugged while an X Window System server is running.

This update adds the following enhancement:

* The wdaemon package has been updated to add the support for Wacom Cintiq DTU-2231 devices. (BZ#713167)

All users of wdaemon are advised to upgrade to this updated package, which adds this enhancement.

1.187. WIRESHARK

1.187.1. RHSA-2011:0370: Moderate wireshark security update

Updated wireshark packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4 and 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.

Wireshark is a program for monitoring network traffic. Wireshark was previously known as Ethereal.

A heap-based buffer overflow flaw was found in Wireshark. If Wireshark opened a specially-crafted capture file, it could crash or, possibly, execute arbitrary code as the user running Wireshark. (CVE-2011-0024)

Several denial of service flaws were found in Wireshark. Wireshark could crash or stop responding if it read a malformed packet off a network, or opened a malicious dump file. (CVE-2010-3445, CVE-2011-0538, CVE-2011-1139, CVE-2011-1140, CVE-2011-1141, CVE-2011-1143)

Users of Wireshark should upgrade to these updated packages, which contain backported patches to correct these issues. All running instances of Wireshark must be restarted for the update to take effect.

1.188. XEN

1.188.1. RHSA-2011:0496: Important xen security update

Updated xen 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. 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 xen packages contain administration tools and the xend service for managing the kernel-xen kernel for virtualization on Red Hat Enterprise Linux.

It was found that the xc_try_bzip2_decode() and xc_try_lzma_decode() decode routines did not correctly check for a possible buffer size overflow in the decoding loop. As well, several integer overflow flaws and missing error/range checking were found that could lead to an infinite loop. A privileged guest user could use these flaws to crash the guest or, possibly, execute arbitrary code in the privileged management domain (Dom0). (CVE-2011-1583)

All xen users are advised to upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

1.188.2. RHBA-2011:1070: xen bug fix and enhancement update

Updated xen packages that fix various bugs and add several enhancements are now available for Red Hat Enterprise Linux 5.

IMPORTANT

This update was released as errata RHBA-2011:1070 — xen bug fix and enhancement update.

The xen packages contain administration tools and the **xend** service for managing the kernel-xen kernel for virtualization on Red Hat Enterprise Linux.

Bug Fixes:

BZ#661927

When a large number, several tens or more, of Virtual Block Devices (VBDs) were present in a guest operating system, the time the **xm create** command took to boot a guest increased for each subsequent guest. With this update, the check procedure for duplicate devices has been optimized to significantly speed up guest creation, and proper XenStore storage space entry transaction handling has been provided, fixing this bug.

BZ#702248

If a guest had 32 GB of operating memory or more, the Desktop Management Interface (DMI) information provided to the guests was incorrect. This was detected by the System Management BIOS (SMBIOS) tests required for the Microsoft Server Virtualization Validation Platform (SVVP) certification. With this update, a patch has been provided, and the DMI information provided to the guests with very large operating memory is now correct.

BZ#702607

Microsoft's Server Virtualization Validation Platform (SVVP) tests detected unreliability of the emulated HPET (High Performance Event Timer) on some hosts. With this update, the HPET can be configured as a per-domain configuration option; if it is disabled, the guest will choose a more reliable timer source. Disabling the HPET is suggested for Windows guests, as well as fully-virtualized Linux guests that show occasional **time went backwards** errors in the console.

BZ#625368

On the Itanium platform, it was possible to create a HVM (Hardware Virtual Machine) guest with more than 32 virtual CPUs (VCPUs) without any warning messages. Consequently, the **xm list** command reported only one VCPU on that machine. With this update, a patch has been provided to disallow HVM guest creation with more than 32 VCPUs on the Itanium platform, as this is not supported, thus preventing this bug.

BZ#630814

Previously, the mouse cursor could not be moved in an fully-virtualized guest when the emulated PS/2 mouse was chosen together with the *Local SDL Window*display method. With this update, a patch has been provided that fixes this incorrect behavior of the PS/2 mouse in an SDL (Simple DirectMedia Layer) window, and the mouse cursor now works as expected.

BZ#637351

When the device_model variable in a HVM guest configuration file was not properly specified, the **qemu-dm** daemon did not start; even though the virtual machine was created, its status reported by the **xm list** command was incorrect, and the machine could not be properly used. With this update, the device model is checked on domain startup and an error message is issued by the xend daemon if the device model is incorrect, thus preventing this bug.

BZ#641541

After a domain name was changed via the **xm rename** command, the **xentop** utility failed to properly reflect this change in its output. With this update, the **setName()** function has been fixed to propagate the new domain name to domain paths and back-end domain names, and **xentop** now shows these changes properly.

BZ#652150

Previously, when the **rename-restart** option was set as a reaction to a guest termination and the **xend** daemon was restarted after the guest crashed, **xend** lost track of the new guest instance. This bug has been fixed, and all guests are now visible via **xend** after the daemon restart.

BZ#658712

Previously, the **xend** daemon did not perform syntax checks for block devices either in configuration files or on the command line. As a consequence, the guest was exposed to a kernel panic or the **xm block-attach** command failed. With this update, a patch has been provided, and **xend** now checks the format of block device entries and parameters before adding the information into XenStore storage space, fixing these issues.

BZ#673456

After a PV (paravirtualized) guest was saved, restored and then destroyed on a disk partition with insufficient space, the **xend** daemon preserved reference to the non-existent guest. As a consequence, a zombie guest sometimes appeared and was reported by the **xm list** command. With this update, a memory leak has been fixed in the **xc_resume()** function, and now no zombie guests appear in the described scenario.

BZ#692034

When a guest was configured with both **xvd[x]** and **hd[x]** disks attached (where [x] is a sequential identifying letter), the disk configured as **xvd[x]** was not recognized. The guest then could fail to boot, reporting no available bootable disk. With this update, Xen fully-virtualized guests show **xvd[x]** disks also as IDE devices, letting guests boot properly in the described scenario.

BZ#605956

Previously, if the virtual CD-ROM was ejected in the guest operating system, and the **xm block-configure** command was subsequently used to reinsert the same medium, the guest operating system failed to detect the newly inserted medium. With this update, a patch has been provided that handles CD-ROM ejection properly, fixing the bug.

BZ#626806

Previously, a 32-bit HVM guest running under a 64-bit hypervisor terminated unexpectedly if the **xm mem-set** command attempted to change the guest's memory reservation. With this update, a patch has been provided that checks whether the HVM domain is 32-bit or 64-bit. The patch then disallows the aforementioned method of setting up memory for guests, thus ensuring this bug can no longer occur.

BZ#627551

When an HVM guest with several disks emulated as SCSI via the QEMU emulator booted, numerous SCSI inquiry errors were returned. With this update, a patch has been provided to properly handle the varying length of the inquiry commands, and the aforementioned error messages are no longer returned.

BZ#638488

Prior to this update, a race condition had been occurring between the **xend** daemon and the **xen-hotplug-cleanup** script, causing the **qemu-dm** utility to terminate with a segmentation fault. With this update, a patch that fixes the race condition in **xend** hot plug scripts has been provided, and the segmentation fault no longer occurs.

BZ#651912

Previously, the cache flush for IDE devices emulated via the **qemu** emulator was performed synchronously. When the flush process took too much time, the virtual CPU was stuck while the **fsync** utility was running. This behavior sometimes caused guests to terminate unexpectedly on the Windows operating system. With this update, cache flushes for IDE devices are done asynchronously, and a crash no longer occurs in the described scenario.

BZ#652310

When initializing PCI devices, due to an off-by-one-bit error in the **hvmloader** BIOS, fully-virtualized Xen guests with more than 12 PCI devices could not be created. This bug has been fixed, and now up to 28 PCI devices can be attached to a fully-virtualized guest.

BZ#657187

When starting or stopping the xendomains service with an invalid image and a regular saved domain, the formatting of the output messages was confusing and hard to read. With this update, the output has been clarified.

BZ#661277

Prior to this update, the hot plug scripts did not check if an image file existed before doing further processing. Consequently, when a non-existent image file was attached to a guest, the output error message was too vague to be helpful. This bug has been fixed, and the error message is sufficiently informative.

BZ#663933

Previously, a random MAC address was generated for dom0 TAP devices in HVM guests. If this address sorted above the MAC address of the bridge interface, the connectivity to the guest was lost. With this update, a dummy MAC address that is always larger than the MAC address of any bridge interface is generated instead, and this bug no longer occurs.

BZ#665011

Memory leaks were discovered in the code following the deletion of block headers and also in the following functions: **`raw_aio_remove()`**, **`qemu_bh_delete()`** and **`pt_msix_init()`**. With this update, a set of patches has been provided to fix these bugs.

BZ#665017

Prior to this update, double click or dragging mouse events were sometimes lost when using an emulated USB mouse or a tablet device in a fully-virtualized guest. With this update, buffering of mouse events has been added to the emulation of USB pointer devices, and lost mouse events occur much less frequently.

BZ#665032

When a Red Hat Enterprise Linux 6.1 fully-virtualized Xen guest requested an unplug of emulated network cards, the **qemu-dm** device model would also disconnect host network cards that were passed-through to the guest. This bug has been fixed, and now the pass-through NICs (Network Interface Cards) remain functioning for Red Hat Enterprise Linux 6.1 guests.

BZ#669388

A part of the recovery code in the **`XendDomain.py`** source file used an unqualified name to access the **`XendDomainInfo.do_FLR()`** function. As a consequence, a network card's virtual functions were not properly reset before a fully-virtualized guest was started. With this update, all **`do_FLR()`**

calls use the correct scope, and this bug no longer occurs.

BZ#674514

The **xenctx** utility compiled on a 64-bit architecture was using the 64-bit version of the `xen_cr3_to_pfn()` function on 32-bit PV and HVM domains. With this update, **xenctx** prints 32-bit register values as expected, fixing this bug.

BZ#675733

When a PV guest was installed via the **grub2** utility, the unprivileged domain (DomU) failed to be created, and the guest failed to boot. With this update, a patch that supports `(hdX, msdosY)` partition syntax for **grub2** has been provided, and the guest is now able to boot successfully in the described scenario.

BZ#680407

Previously, the **blktap** user-space component did not support attaching more than 100 devices to a guest. With this update, a patch has been provided to address this issue, and now up to 255 image files can be properly attached to a guest.

BZ#683437

Previously, version 2.6.38 or newer kernels, which are compressed using the **xz** compression utility, could not be properly booted with the xen package. With this update, **xz** decompression support has been added, thus fixing this bug.

Enhancements:

BZ#614004

This update introduces a feature to export two or more serial ports to a Xen guest.

All users of xen are advised to upgrade to these updated packages, which provide numerous bug fixes and an enhancement.

1.188.3. RHBA-2011:0342: xen bug fix update

Updated xen packages that fix various bugs are now available for Red Hat Enterprise Linux 5 Extended Update Support.

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.

This update fixes the following bugs:

* With a large number of virtual block devices (VBDs) or virtual guests, looking for duplicate devices could take a very long time and significantly increase overall boot time. With this update, this procedure has been optimized not to require XenStore, so that virtual guests now boot much faster. Additionally, this update also ensures that the domain record counter contains a correct value when a XenStore transaction is canceled. Note that when you add a network interface controller (NIC) with an automatically generated MAC address, this address is not verified. Avoid using a combination of hard-coded and automatically assigned MAC addresses, as this can lead to a guest network failure. (BZ#666802)

* Previously, creating a new domain caused a hot plug script to perform an additional check of disk

sharing capabilities. With a large number of virtual block devices (VBDs), this operation could take a long time, and an attempt to create a new domain could fail due to a timeout. Since a similar checking mechanism is already implemented in the xend service, this update removes this algorithm from the hot plug script, so that it no longer causes a domain creation to fail. (BZ#680928)

Users of xen are advised to upgrade to these updated packages, which resolve these issues. Note that after installation, the xend service must be restarted for this update to take effect.

1.188.4. RHBA-2011:0940: xen bug fix update

Updated xen packages that fix a bug are now available for Red Hat Enterprise Linux 5.

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.

This update fixes the following bug:

* Previously, the cache flush for IDE devices emulated via the QEMU emulator was performed synchronously. When the flush process took too much time, the virtual CPU was stuck while the fsync utility was running. This behavior sometimes caused guests to terminate unexpectedly on the Windows operating system. With this update, cache flushes for IDE devices are done asynchronously, and the crash no longer occurs in the described scenario. (BZ#712412)

Users of xen are advised to upgrade to these updated packages, which fix this bug. Note that after installation, the xend service must be restarted for this update to take effect.

1.189. XINETD

1.189.1. RHBA-2011:0827: xinetd bug fix update

An updated xinetd package that fixes several bugs is now available.

The xinetd daemon is a secure replacement for inetd, the Internet services daemon. It provides access control for all services based on the address of the remote host and/or on time of access, and can prevent denial of service attacks.

This update fixes the following bugs:

* The xinetd.log man page was in the wrong man section, and has been moved to the correct one. The command "man 5 xinetd.log" now works as expected. (BZ#428811)

* When a log file of an xinetd-controlled service exceeded the size limit specified in its configuration file, xinetd terminated unexpectedly with a segmentation fault. With this update, a patch has been applied to address this issue, and the xinetd daemon no longer crashes. (BZ#438986)

* The xinetd.init script did not set its return value correctly when invoked with the "status" argument. This update fixes this issue by making the xinetd.init script return values compatible with Linux Standard Base Core Specification 3.2. (BZ#498119)

* Under certain circumstances the xinetd daemon could hang (for example, when trying to acquire an already acquired lock for writing to its log file) when an unexpected signal arrived. As of this update the daemon handles unexpected signals as expected and the hangs no longer occur. (BZ#501604)

* The xinetd daemon ignored the "port" line of the service configuration file, so it was impossible to bind some rpc services to a specific port. This update addresses this issue and the xinetd daemon now handles the port number appropriately. (BZ#624800)

* This update includes a patch that fixes the compiler warning "dereferencing type-punned pointer will break strict-aliasing rules". (BZ#695674)

All xinetd users are advised to upgrade to this updated package, which addresses these bugs.

1.190. XMLSEC1

1.190.1. RHSA-2011:0486: Moderate xmlsec1 security and bug fix update

Updated xmlsec1 packages that fix one security issue and one bug are now available for Red Hat Enterprise Linux 4 and 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.

The XML Security Library is a C library based on libxml2 and OpenSSL that implements the XML Digital Signature and XML Encryption standards.

A flaw was found in the way xmlsec1 handled XML files that contain an XSLT transformation specification. A specially-crafted XML file could cause xmlsec1 to create or overwrite an arbitrary file while performing the verification of a file's digital signature. (CVE-2011-1425)

Red Hat would like to thank Nicolas Grégoire and Aleksey Sanin for reporting this issue.

This update also fixes the following bug:

* xmlsec1 previously used an incorrect search path when searching for crypto plug-in libraries, possibly trying to access such libraries using a relative path. (BZ#558480, BZ#700467)

Users of xmlsec1 should upgrade to these updated packages, which contain backported patches to correct these issues. After installing the update, all running applications that use the xmlsec1 library must be restarted for the update to take effect.

1.191. XORG-X11-DRV-ATI

1.191.1. RHBA-2011:1008: xorg-x11-drv-ati bug fix update

An updated xorg-x11-drv-ati package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The xorg-x11-drv-ati package provides a driver for ATI cards for the X.Org implementation of the X Window System.

This updated xorg-x11-drv-ati package fixes the following bug:

* Installing Red Hat Enterprise Linux did not successfully complete on HP Workstation Z400, Z600 and Z800 workstations which also used ATI FirePro V5700 or V7750 graphics cards. Due to the X server not supporting DisplayPort, the screen went black after the media check and users were therefore not able to interact with the installation. This problem has been fixed and Red Hat Enterprise Linux can now be successfully graphically installed using DisplayPort. (BZ#568846)

Users of xorg-x11-drv-ati are advised to upgrade to this updated package, which resolves this bug.

1.192. XORG-X11-DRV-MGA

1.192.1. RHEA-2011:0972: xorg-x11-drv-mga enhancement update

An enhanced xorg-x11-drv-mga package is now available for Red Hat Enterprise Linux 5.

The xorg-x11-drv-mga package provides the mga video driver for the X Window System.

This updated xorg-x11-drv-mga package adds the following enhancements:

* The IMMv2 system management controller for integrated MatroxG200eR chipsets is now supported. (BZ#651468)

* With this update, the latest Matrox mga driver is included, and MatroxG200eH chipsets are now supported. (BZ#656962)

* The driver now provides support for Matrox graphic controllers included in Dell PowerEdge servers. (BZ#661286)

All users of xorg-x11-drv-mga are advised to upgrade to this updated package, which adds these enhancements.

1.193. XORG-X11-DRV-QXL

1.193.1. RHBA-2011:1051: xorg-x11-drv-qxl bug fix update

An updated xorg-x11-drv-qxl package that fixes two bugs is now available Red Hat Enterprise Linux 5.

The xorg-x11-qxl-drv package provides 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 (Kernel-based Virtual Machine) and the machine emulator QEMU with the Simple Protocol for Independent Computing Environments (SPICE).

This update fixes the following bugs:

* Prior to this update, only a limited number of resolution choices were available for xql drivers inside the guest, none exceeded 1024x768 in size. To achieve a higher resolution the xorg.conf configuration file had to be manually edited. With this update larger resolutions are provided for guests with appropriate hardware. (BZ#581841)

* Prior to this update, the X server unexpectedly aborted with a segmentation fault and the GNOME Display Manager (GDM) respawned if trying to switch to a virtual console with a key combination in certain circumstances. Now, switching to a virtual console and back to the graphical desktop works as expected. (BZ#585141)

All users of KVM-based virtualization are advised to upgrade to this updated package, which fixes these bugs.

1.194. XORG-X11-DRV-VESA

1.194.1. RHBA-2011:0973: xorg-x11-drv-vesa bug fix update

An updated xorg-x11-drv-vesa package that fixes a bug is now available for Red Hat Enterprise Linux 5.

The xorg-x11-drv-vesa package provides the X.Org X Windows System 11 vesa video driver.

This updated xorg-x11-drv-vesa package fixes the following bug:

* Prior to this update, the native screen resolution (1366x768) could not be set on Dell Precision M4500 Mobile Workstation laptop models when using the vesa video driver. This problem is caused by VBIOS limitations due to its inability to work with floating point numbers. This issue has been fixed: the next closest VBIOS supported screen resolution (1360x768) can now be used for Dell M4500 laptop models. (BZ#614960)

All users of xorg-x11-drv-vesa are advised to upgrade to this updated package, which resolves this issue.

1.195. XORG-X11-FONT-UTILS

1.195.1. RHBA-2011:0418: xorg-x11-font-utils bug fix update

An updated xorg-x11-font-utils package that fixes one bug is now available for Red Hat Enterprise Linux 5.

X.Org is an open source implementation of the X Window System, which provides the basic low-level functionality that full-fledged graphical user interfaces are designed upon. This package provides utilities required to install, convert, and generate fonts.

This update fixes the following bug:

* The Filesystem Hierarchy Standard (FHS) specifies that if the /usr/X11R6/bin/ directory exists, /usr/bin/X11 must be a symbolic link to this directory. Previous versions of the package did not create this symbolic link. With this update, this error has been fixed, and /usr/bin/X11 is now created as expected. (BZ#405891)

All users of xorg-x11-font-utils are advised to upgrade to this updated package, which fixes this bug.

1.196. XORG-X11-SERVER

1.196.1. RHBA-2011:0456: xorg-X11-server bug fix update

Updated xorg-X11-server packages that fix three bugs are now available for Red Hat Enterprise Linux 5.

X.Org is an open source implementation of the X Window System. It provides the basic low-level functionality that full-fledged graphical user interfaces are designed upon.

This update fixes the following bugs:

* Prior to this update, running the X.Org server with the support for backing store enabled (the "backingstore" option) caused the server to occasionally terminate with a segmentation fault. With this update, the underlying source code has been modified to address this issue, and enabling the "backingstore" option in the server's configuration no longer leads to unexpected crashes. (BZ#690270)

* When running the X.Org server with the "r500" video driver, an attempt to use the system-config-display utility to enable dual head mode with the "Desktop layout" option set to "Individual Desktops"

could render a user unable to move the mouse pointer between the screens. This update corrects this error, and the use of the "Individual Desktops" option no longer confines the mouse pointer to a single screen. (BZ#694728)

* Due to an error in the X.Org server, a user may have been occasionally unable to move the mouse pointer outside the area near the left edge of the screen. With this update, a patch has been applied to correct this error, and users are now always allowed to move the mouse pointer around the screen as expected. (BZ#695252)

All users of xorg-x11-server are advised to upgrade to these updated packages, which fix these bugs.

1.197. XORG-X11-SERVER-UTILS

1.197.1. RHSA-2011:0433: Moderate xorg-x11-server-utils security update

An updated xorg-x11-server-utils package that fixes one security issue is now available for Red Hat Enterprise Linux 5 and 6.

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 xorg-x11-server-utils package contains a collection of utilities used to modify and query the runtime configuration of the X.Org server. X.Org is an open source implementation of the X Window System.

A flaw was found in the X.Org X server resource database utility, xrdb. Certain variables were not properly sanitized during the launch of a user's graphical session, which could possibly allow a remote attacker to execute arbitrary code with root privileges, if they were able to make the display manager execute xrdb with a specially-crafted X client hostname. For example, by configuring the hostname on the target system via a crafted DHCP reply, or by using the X Display Manager Control Protocol (XDMCP) to connect to that system from a host that has a special DNS name. (CVE-2011-0465)

Red Hat would like to thank Matthieu Herrb for reporting this issue. Upstream acknowledges Sebastian Krahmer of the SuSE Security Team as the original reporter.

Users of xorg-x11-server-utils should upgrade to this updated package, which contains a backported patch to resolve this issue. All running X.Org server instances must be restarted for this update to take effect.

1.197.2. RHBA-2011:0454: xorg-x11-server-utils bug fix update

An updated xorg-x11-server-utils package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The xorg-x11-server-utils package contains a collection of utilities used to modify and query the runtime configuration of the X.Org server. X.Org is an open source implementation of the X Window System.

This update fixes the following bug:

* A previous advisory, the RHSA-2011:0433 xorg-x11-server-utils security update, applied a backported patch to fix a flaw in the X server resource database utility, xrdb. While this patch resolved the security issue, it also introduced an error in the macro expansion mechanism. Consequent to this, an attempt to run the xrdb utility could fail with the following messages written to standard error:

sh: -c: line 0: unexpected EOF while looking for matching `"' sh: -c: line 1: syntax error: unexpected end of file

With this update, the underlying source code has been adapted to correct the macro expansion mechanism, and the xrdb utility now works as expected. (BZ#696316)

All users of xorg-x11-server-utils are advised to upgrade to this updated package, which fixes this bug. Note that all running instances of the X.Org server must be restarted for this update to take effect.

1.198. XORG-X11-XFS

1.198.1. RHBA-2011:0457: xorg-x11-xfs bug fix update

Updated xorg-x11-xfs packages that resolve an issue are now available for Red Hat Enterprise Linux 5.

The X.Org X11 xfs font server provides a standard mechanism for an X server to communicate with a font renderer.

These updated xorg-x11-xfs packages fix the following bug:

* Prior to this update, the X Window System font server (xfs) could have terminated with a segmentation fault on 64-bit platforms if the client-limit was set to values greater than 100. With this update, the underlying code has been changed and xfs remains stable regardless of the set client limit. (BZ#685065)

All users of xorg-x11-xfs are advised to upgrade to these updated packages, which resolve this issue.

1.199. YABOOT

1.199.1. RHBA-2011:0993: yaboot bug fix update

An updated yaboot package that fixes three bugs is now available for Red Hat Enterprise Linux 5.

The yaboot package provides a boot loader for Open Firmware based PowerPC systems. It can be used to boot IBM eServer System p machines.

This update fixes the following bugs:

* Prior to this update, the /etc/yaboot.conf parser failed during install when the quoted string was too long. This update modifies the code to significantly extend the size of quoted strings. Now, the /etc/yaboot.conf file parses as expected. (BZ#579834)

* Prior to this update, attempting to load a kernel with the CONFIG_RELOCATABLE option failed with the error message that no valid ELF image was found. With this update, the underlying code has been modified to allow this format. Now, relocatable kernel images can be loaded as expected. (BZ#645756)

* Prior to this update, the boot prompt caused characters to disappear when the label name was pasted in. This updated package corrects the boot prompt. Now, even very long names can be pasted in. (BZ#659403)

All users of yaboot are advised to upgrade to this updated package, which fixes these bugs.

1.200. YPBIND

1.200.1. RHBA-2011:0912: ypbind bug fix update

An updated ypbind package that fixes a bug is now available for Red Hat Enterprise Linux 5.

The ypbind package provides an NIS (Network Information Services) daemon which binds NIS clients to an NIS domain.

This update fixes the following bug:

* Each NIS client can bind to different NIS servers, but can only be bound to one server at a time. To maintain its connection to a server, an NIS client checks connection to an active server every 20 seconds and once in a while tries to find the fastest available server. Previously, clients searched for the fastest server every minute, which sometimes caused heavy traffic and response delays. With this update, clients search for the fastest server every 15 minutes, preventing this bug. (BZ#714028)

All users of ypbind are advised to upgrade to this updated package, which fixes this bug.

1.201. YPSERV

1.201.1. RHBA-2011:0444: ypserv bug fix update

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

The Network Information Service (NIS) is a system that provides network information (login names, passwords, home directories, group information) to all of the machines on a network.

This updated ypserv package fixes the following bug:

* Due to a string concatenation error in the code, running the "yppasswdd" command and using the "-x" option, which instructs yppasswdd to pass data to an external program to update the source files and maps, could have caused garbage characters to be inserted in front of the username, thus causing the output to become unparseable. This has been resolved in this updated package by changing the operation to a string-copy, with the result that the username is no longer corrupted when using the "-x" option. (BZ#688237)

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

1.202. YUM

1.202.1. RHBA-2011:1060: yum bug fix update

An updated yum package that fixes several bugs is now available for Red Hat Enterprise Linux 5.

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.

This update fixes the following bugs:

* When accessing mirror lists, a number of yum configuration options was not correctly recognized by the yum utility or associated modules such as URLGrabber. As a consequence, many configured parameters were not taken into account during yum operation; for example, the timeout option was ignored, causing unpredictable timeouts. This bug has been fixed, and the yum configuration is now properly processed by yum and associated modules. (BZ#647134)

* Previously, when one of the repository baseurl addresses caused an HTTP error code to be issued, the "yum repolist" command failed to produce the list of available repositories. This bug has been fixed and the repository list is now properly returned even if an error occurs. (BZ#697087)

* Previously, the repodiff utility used a stale metadata cache in subsequent runs. When two repodiff commands were executed in succession, the second run reused cached data from the first. This bug has been fixed and repodiff now properly validates the metadata if a connection cannot be established or the cached data are about to be reused. (BZ#709972)

* One of the arguments in the ssl_ctx_load_verify_locations() function was of the wrong type. As a consequence, under specific conditions, any yum command could terminate with a traceback. A patch has been provided to address this issue, and the yum utility no longer crashes in the described scenario. (BZ#712896)

Users of yum are advised to upgrade to this updated package, which fixes these bugs.

1.203. YUM-RHN-PLUGIN

1.203.1. RHBA-2011:0998: yum-rhn-plugin bug fix update

An updated yum-rhn-plugin package that fixes various bugs is now available for Red Hat Enterprise Linux 5.

The yum-rhn-plugin package provides support for connecting to Red Hat Network (RHN). Systems registered with RHN are able to update and install packages from Red Hat Network.

This update fixes the following bugs:

* When running the "yum --help" command with rhnplugin installed, command line options for other plug-ins were not listed in the output, although the plug-in options were still working. This error has been corrected: plug-in options are now listed. (BZ#614138)

* Due to rhnplugin not considering the value of Yum's "metadata_expire" variable, all channels used the default expiration time (21,700 seconds). This prevented a user from updating a system using RHN Satellite. rhnplugin now respects Yum's global settings. (BZ#666534)

* When using RHN Classic or RHN Satellite to schedule an installation or update on the client system with outdated Yum's metadata cache, the "rhn_check" utility incorrectly reported success. This error has been fixed and the scheduled action fails if Yum does not find any new packages to install or update. (BZ#667135)

* When a system registered by the Subscription Manager tool was updated with Yum and rhnplugin was enabled, the following message appeared:

This system is not registered with RHN. RHN support will be disabled.

The problem has been fixed: rhnplugin is now disabled by default, and is only enabled when registering with RHN Classic. If the system is registered with Subscription Manager, rhnplugin is not used and the message does not appear. (BZ#675220)

* The version of yum-rhn-plugin released with Red Hat Enterprise Linux 5.7 Beta did not print the progress bar during the download of packages. This has been fixed by correctly setting callbacks. (BZ#707241)

All users of yum-rhn-plugin are advised to upgrade to this updated package, which fixes these bugs.

1.203.2. RHBA-2011:0331: yum-rhn-plugin bug fix update

An updated yum-rhn-plugin package that fixes a bug is now available for Red Hat Enterprise Linux 5.

Red Hat Network Client Tools provide programs and libraries that allow a system to receive software updates from Red Hat Network (RHN). yum-rhn-plugin allows yum to access a Red Hat Network server for software updates.

This updated yum-rhn-plugin package fixes the following bug:

* The rhnplugin provided by the yum-rhn-plugin package did not respect yum's metadata_expire setting, and therefore all RHN or RHN Satellite channels used the default expiration time of 6 hours. With this updated package, rhnplugin now respects the relevant settings from the /etc/yum.conf configuration file, including the metadata_expire directive. (BZ#681137)

All users of yum-rhn-plugin are advised to upgrade to this updated package, which resolves this issue.

1.204. YUM-UTILS

1.204.1. RHBA-2011:1045: yum-utils bug fix and enhancement update

Updated yum-utils packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

The yum-utils package contains a collection of utilities written by various authors for the Yum package manager, as well as usage examples. The utilities provided by yum-utils make Yum more powerful and easier to use.

These updated yum-utils packages provide fixes for the following bugs:

* Prior to this update, if "yum update" failed and the user ran the "yum-complete-transaction" program, the program offered to delete system critical packages. With this update, the program obtains the list of failed yum transactions and finishes the transactions without removing any packages critical for the system's operation. (BZ#495911)

* In accordance with current guidelines, all Python executables have been updated to use the "#!/usr/bin/python" bang line instead of "#!/usr/bin/env python". (BZ#521905)

* Prior to this update, the repodiff utility could have experienced performance issues. This was caused by an inefficient algorithm used for comparing packages. This update improves the repodiff algorithm by making it more efficient. (BZ#646571)

* Prior to this update, the repodiff utility could not handle packages with descriptions that contained non-ASCII characters, and could have failed to set up repositories with such summaries. With this update, the utility handles the characters correctly and works as expected on repositories with packages containing non-ASCII characters. (BZ#647521)

* Prior to this update, the yum-groups-manager utility could have returned a python traceback when loading group metadata from a gzipped file. This occurred because it used an incorrect argument when opening the gzipped file. With this update, the underlying code has been changed and the gzipped file is opened correctly. (BZ#648623)

* Prior to this update, the repoquery utility could not handle packages with descriptions that contained non-ASCII characters. With this update, the utility handles the characters correctly and works as expected on repositories containing packages which use non-ASCII characters. (BZ#702282)

In addition, these updated packages provide the following enhancements:

* This update adds the yum-plugin-priorities package, which provides the yum priority feature. This allows the user to set a precedence of one repository over another. (BZ#518129)

* With this update, the repodiff utility can override the global excludes set in the yum.conf configuration file. (BZ#643137)

Users are advised to upgrade to these updated yum-utils packages, which resolve these issues and add these enhancements.

1.205. ZLIB

1.205.1. RHBA-2011:0503: zlib bug fix update

An updated zlib package that fixes two bugs is now available for Red Hat Enterprise Linux 5.

Zlib is a general-purpose lossless data compression library that is used by many different programs.

This update fixes the following bugs:

* When used to combine two Adler-32 checksums, the adler32_combine() function could occasionally produce an incorrect result. With this update, an upstream patch has been applied to fix the underlying algorithm, and the adler32_combine() function no longer returns incorrect checksums. (BZ#622779)

* Previous versions of the zlib package installed shared libraries to the /usr/lib directory (on 64-bit systems, also in /usr/lib64). Consequent to this, when the /usr directory was on a separate partition, certain applications may have been unable to start before this partition was mounted. This update changes the installation target for these libraries to /lib (and /lib64 on 64-bit systems) to ensure that these libraries are available before /usr is mounted. For compatibility reasons, the /usr/lib directory (on 64-bit systems, also /usr/lib64) now contains symbolic links to these libraries. (BZ#678352)

All users are advised to upgrade to this updated package, which fixes these bugs.

CHAPTER 2. NEW PACKAGES

New Packages

2.1. RHEA-2011:0944: NEW PACKAGES: BNX2X-KMOD, BNX2I-KMOD, BNX-KMOD, CNIC-KMOD

New bnx2x-kmod, bnx2i-kmod, bnx2-kmod and cnic-kmod packages are now available for Red Hat Enterprise Linux 5.

These packages provide kernel modules for controlling Broadcom NetXtreme II network devices. Beyond what was delivered in Red Hat Enterprise Linux 5, temporary drivers are now available for the following hardware:

Broadcom NetXtreme II 5771x 10Gigabit Ethernet Broadcom NetXtreme II BCM5706/5708/5709/5716 Broadcom NetXtreme II BCM5706/5708/5709/57710/57711/57712 iSCSI Broadcom NetXtreme II CNIC

This update adds the following enhancements:

The bnx2x-kmod-1.62.00_6-1.el5_6 package is a temporary driver update released as part of the Red Hat Enterprise Linux Driver Update Program (DUP). (BZ#707448)

The bnx2i-kmod-2.6.2.3-2.el5_6 package is a temporary driver update released as part of the Red Hat Enterprise Linux Driver Update Program (DUP). (BZ#712473)

The bnx2-kmod-2.0.21-2.el5_6 package is a temporary driver update released as part of the Red Hat Enterprise Linux Driver Update Program (DUP). (BZ#712470)

The cnic-kmod-2.2.13-2.el5_6 package is a temporary driver update released as part of the Red Hat Enterprise Linux Driver Update Program (DUP). (BZ#712475)

Only users requiring temporary driver support for the specific hardware noted above should install these packages. Unless a system contains the exact hardware the above packages explicitly support, these packages must not be installed.

2.2. RHEA-2011:0985: NEW PACKAGE: BUILDSYS-MACROS

A new buildsys-macros package is now available for Red Hat Enterprise Linux 5.

The buildsys-macros package provides macros for building Red Hat Enterprise Linux packages.

This new package adds buildsys-macros to Red Hat Enterprise Linux 5. (BZ#613985)

All users who require buildsys-macros are advised to install this new package.

2.3. RHEA-2011:0995: NEW PACKAGE: CMAKE

A new cmake package is now available for Red Hat Enterprise Linux 5.

CMake is an open source, cross-platform build system that is used to control the software compilation process using simple platform- and compiler-independent configuration files. CMake generates native makefiles and workspaces that can be used in the compiler environment of your choice.

This enhancement update adds the cmake package to Red Hat Enterprise Linux 5. (BZ#673914)

All users who require cmake should install this new package.

2.4. RHEA-2011:0974: NEW PACKAGES: DING-LIBS

New ding-libs packages are now available for Red Hat Enterprise Linux 5.

The ding-libs packages contain the "Ding is not GLib" assorted utility libraries, which provide libcollection, libini_config, libdhash and libref_array for use with SSSD and related projects.

This enhancement update adds the ding-libs packages to Red Hat Enterprise Linux 5. (BZ#665312, BZ#677753)

All users who require SSSD are advised to install these new packages.

2.5. RHEA-2011:0970: NEW PACKAGE: IWL5150-FIRMWARE

An iwl5150-firmware package that matches the iwlagn driver in Red Hat Enterprise Linux kernels is now available.

The iwlagn driver requires firmware loaded on the Intel Wireless WiFi Link 5150AGN series adapter device to operate correctly. This package provides the required firmware.

This enhancement update provides the firmware required by the iwlagn driver. (BZ#559269)

All users who require iwl5150-firmware are advised to install this new package.

2.6. RHEA-2011:1052: NEW PACKAGES: LIBCXGB4

New libcxgb4 packages are available for Red Hat Enterprise Linux 5.

libcxgb4 provides a userspace hardware driver for use with the libibverbs InfiniBand/iWARP verbs library. This driver enables Chelsio Internet Wide Area RDMA Protocol (iWARP) capable Ethernet devices.

* This enhancement update adds the libcxgb4 package to Red Hat Enterprise Linux 5. (BZ#693511)

All users of Chelsio iWARP capable Ethernet devices are advised to install these new packages.

2.7. RHEA-2011:1009: NEW PACKAGE: MAN-PAGES-OVERRIDES

A new man-pages-overrides package is now available for Red Hat Enterprise Linux 5.

The man-pages-overrides package contains a collection of manual ("man") pages to complement other packages or update those contained therein.

This enhancement update adds the man-pages-overrides package to Red Hat Enterprise Linux 5. (BZ#558469)

Among other changes, this new package fixes the following manual pages issues:

* A typo in the crontab(1) manual page has been fixed. (BZ#448544)

* A reference to the nonexistent pacct(5) manual page in the sa(8) manual page has been removed. (BZ#464865)

* Missing pnmtojbig(1) and pcdovtoppm(1) manual pages have been added. (BZ#496036)

* The mount(8) man page now contains missing information about the ext4 and XFS file systems. (BZ#536899)

* The sh(1) man page now contains fixed information about the default value of the PATH variable. (BZ#576795)

* The expect(1) man page formatting issue has been fixed. (BZ#633696)

* The ypserv(8), rpc.yppasswdd(8) and rpc.ypxfrd(8) manual pages now contain information about the possibility of setting internal options. (BZ#656438)

* A typo in the cron(8) manual page has been fixed. (BZ#658860)

* The route(8) manual page now includes an explicit description of the "mss M" option. (BZ#671321)

* The unsupported keyword "order" has been removed from the host.conf(5) manual page. (BZ#698153)

* The path to the cifs.upcall program has been corrected in the cifs.upcall(8) manual page, and the nounix option description has been added to the mount.cifs(8) manual page. (BZ#621926)

* The ldap.conf(5) manual page has been modified in order to prefer usage of the TLS_CACERT option instead of the TLS_CACERTDIR option to specify Certificate Authorities. (BZ#649048)

All users should install this new man-pages-overrides package.

2.8. RHEA-2011:0989: NEW PACKAGE: OPENLDAP24-LIBS

A new openldap24-libs package is now available for Red Hat Enterprise Linux 5.

The openldap24-libs package contains OpenLDAP 2.4 client libraries.

This enhancement update adds the openldap24-libs package to Red Hat Enterprise Linux 5. (BZ#658238)

All users who require openldap24-libs should install this new package.

2.9. RHEA-2011:1004: NEW PACKAGES: OPENSCAP

New openscap packages are now available for Red Hat Enterprise Linux 5.

The openscap packages provide a set of open source libraries for the integration of Security Content Automation Protocol (SCAP). SCAP is a set of standards that provide a standard language for the expression of Computer Network Defense related information.

This new package adds OpenSCAP to Red Hat Enterprise Linux 5. (BZ#682207)

All users who require OpenSCAP are advised to install these new packages.

2.10. RHEA-2011:0991: NEW PACKAGE: PERL-NETADDR-IP

A new perl-NetAddr-IP package is now available for Red Hat Enterprise Linux 5.

The perl-NetAddr-IP module provides an object-oriented abstraction on top of IP addresses or IP subnets, that allows for easy manipulations.

This new package adds perl-NetAddr-IP to Red Hat Enterprise Linux 5. (BZ#524225)

Note: this new packages is added as an dependency of the spamassassin package.

All users who require perl-NetAddr-IP are advised to install this new package.

2.11. RHEA-2011:1014: NEW PACKAGE: PYTHON-ETHTOOL

A new python-ethtool package is now available for Red Hat Enterprise Linux 5.

The python-ethtool package makes the ethtool kernel interface available within the Python programming environment to allow querying and changing of Ethernet card settings, such as speed, port, auto-negotiation, and PCI locations.

This new package adds python-ethtool to Red Hat Enterprise Linux 5. (BZ#675232)

All users who require python-ethtool are advised to install this new package.

2.12. RHEA-2011:1077: NEW PACKAGE: PYTHON-RHSM

A new python-rhsm package is now available for Red Hat Enterprise Linux 5.

The python-rhsm package provides access to the Subscription Management tools. It helps users to understand specific products which are installed on their machines and specific subscriptions which their machines consume.

This enhancement update adds a new python-rhsm package to Red Hat Enterprise Linux 5. (BZ#661863)

All users requiring python-rhsm should install this newly-released package, which adds this enhancement.

2.13. RHEA-2011:1013: NEW PACKAGE: PYTHON-SIMPLEJSON

A new python-simplejson package is now available for Red Hat Enterprise Linux 5.

The python-simplejson package implements efficient JSON encoding and decoding for the Python programming environment.

This enhancement update adds the python-simplejson package to Red Hat Enterprise Linux 5. (BZ#675233)

All users who require python-simplejson are advised to install this new package.

2.14. RHEA-2011:1006: NEW PACKAGE: PYTHON-SUDS

A new python-suds package is now available for Red Hat Enterprise Linux 5.

The python-suds package provides a lightweight implementation of the Simple Object Access Protocol (SOAP) for the Python programming environment.

This enhancement update adds the python-suds package to Red Hat Enterprise Linux 5. (BZ#681834)

All users who require python-suds are advised to install this new package.

2.15. RHEA-2011:1078: NEW PACKAGES: SUBSCRIPTION-MANAGER

New subscription-manager packages that provide GUI and command line tools for the new Subscription Manager system are now available for Red Hat Enterprise Linux 5.

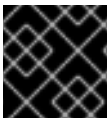
The new Subscription Management tooling will allow users to understand the specific products which have been installed on their machines, and the specific subscriptions which their machines are consuming.

This enhancement update adds new subscription-manager packages to Red Hat Enterprise Linux 5. (BZ#668616)

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

2.16. RHBA-2011:1072: NEW PACKAGE: TCSH617

A new tcsh617 package, a replacement for the tcsh package that, among other fixes and enhancements, addresses various bugs of the tcsh package, is now available for Red Hat Enterprise Linux 5.



IMPORTANT

This update was released as errata RHBA-2011:1072 – new package: tcsh617.

Tcsh is a command language interpreter compatible with the *C* shell (**csh**), which can be used as an interactive login shell, as well as a shell script command processor.

This new tcsh617 package serves as a replacement for the tcsh package, and upgrades **tcsh** to upstream version 6.17, which incorporates a number of bug fixes and enhancements over the previous version (6.14), which was released as a part of Red Hat Enterprise Linux 5.5. The tcsh package has been retained for compatibility with the older version of **tcsh**.

The tcsh and tcsh617 packages are mutually-exclusive: both packages cannot be installed simultaneously. Users of **tcsh** who require the bug fixes and enhancements included in this upgraded package are advised to first uninstall the tcsh package and then install this new tcsh617 package. (BZ#676136)

Bug Fixes:

BZ#676136

The **tcsh** shell used to call **malloc()**-related functions inside signal handlers. This could cause **tcsh** to become unresponsive due to calling just-interrupted internal **glibc** locking algorithms again. Operations related to **malloc()** were moved from signal handlers to common routines.

BZ#433908

Previously, the **tcsh(1)** man page stated that the shell would not run a set-user ID script without an **-b** argument. This statement was removed from the man page because it is forbidden to run set-user ID scripts in Red Hat Enterprise Linux 5.

BZ#436439

Prior to this update, the **tcsh(1)** man page inaccurately stated that it is mandatory to use the **group** option when using the **newgrp** built-in command. The corrected statement now says that using **group** is optional.

BZ#436901

Previously, the **tcsh** shell allowed to name variables in incorrect formats, such as by beginning a variable name with a digit. This issue has been fixed: variable names are now verified according to Unix variable-naming conventions.

BZ#437079, **BZ#437080**

The **tcsh(1)** man page inaccurately stated that the **hup** and **nohup** built-in commands, when used without an argument, can be used only within a shell script. The man page has been corrected: it now states that the **hup** and **nohup** built-in commands can be used when running the shell non-interactively.

BZ#618723

When **tcsh** did not exit properly, it could have entered an infinite loop, using 100% of the CPU, and become unresponsive. This was caused by a function interrupting the exit routine and then re-entering the code and thus causing it to loop infinitely.

BZ#638955

This package fixes the return value of the **status** (or **$?**) variable in the case of pipelines and backquoted commands. The **anyerror** variable, which selects behavior, has been added to retain the backward compatibility.

BZ#650363

When **tcsh** evaluated a backquoted command (using command substitution) which itself contained backquotes, it could have dumped core due to a buffer overflow. With this update, nested command substitutions are now handled correctly, and **tcsh** no longer dumps core in this situation.

BZ#676305

Previously, when the **LANG** environment variable was set to **C**, the **tcsh** shell could ignore several characters that were following a wide (greater than 8 bits) character while receiving user's input. This package fixes the issue and **tcsh** no longer ignores any characters.

BZ#688170

Previously, when a command was substituted using backquotes, a second, redundant **fork()** system call was performed. This could have caused problems when a child process needed to find the PID of its **tcsh** parent. With this new package, only one **fork()** is performed.

BZ#688173

Previously, running **tcsh** in verbose mode caused the shell to append history to its output on exit. This new package fixes the issue and **tcsh** now works as expected.

BZ#688175

On a local machine, **tcsh** set the **REMOTEHOST** environment variable to an empty string, even though this variable should only have been set on a remote machine. This error has been fixed and **REMOTEHOST** is no longer set on a local machine.

BZ#689381

Previously, if the **printexitvalue** variable was set, **tcsh** returned the exit code number as a part of the command output, rendering the output unusable. This has happened due to a missing job status flag. The proper flag has been set and the command output is now correct.

BZ#689382

Previously, under certain circumstances, a null pointer may have been incorrectly dereferenced, causing the **tcsh** shell to terminate unexpectedly. With this update, the pointer is now tested for the **NULL** value before it is dereferenced, and **tcsh** no longer crashes in this circumstance.

BZ#690500

The **tcsh** shell entered an infinitive loop when standard output was redirected to a child process by a pipe. When the child process was terminated, **tcsh** tried to print a message to the already-closed pipe as a high-priority event that could never finish. This has been fixed so in case that such child process terminates, the relevant error event is removed from the event queue before it could have been written to the broken pipe, and the parent process is terminated as well.

All users of the tcsh package who want to upgrade their version of tcsh to 6.17 are advised to uninstall the tcsh package and then install this upgraded tcsh617 package, which provides these bug fixes and enhancements.

2.17. RHEA-2011:1015: NEW PACKAGE: VIRT-WHAT

A new virt-what package is now available for Red Hat Enterprise Linux 5.

The virt-what tool is used to detect whether the operating system is running inside a virtual machine.

This enhancement update adds a new virt-what package to Red Hat Enterprise Linux 5. The virt-what utility enables programs to detect if they are running in a virtual machine, as well as details about the type of hypervisor. (BZ#668618)

All users requiring virt-what should install these newly-released package, which adds this enhancement.

CHAPTER 3. 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.

DFS

Starting with Red Hat Enterprise Linux 5.3, CIFS supports Distributed File System (DFS) as a Technology Preview.

CDTB

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.

Brocade BFA Fibre-Channel/FCoE driver

the **bfa** driver for Brocade Fibre Channel Host Bus adapters is considered a Technology Preview in Red Hat Enterprise Linux 5.7. (BZ#475695)

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/.

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, included as a Technology Preview, 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 join the stateless-list@redhat.com mailing list.

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.

- 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.

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.

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**.

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 Technology Preview in Red Hat Enterprise Linux 5.7.

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/open-

fcoe/wiki/quickstart.

Red Hat Enterprise Linux 5.7 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 **mthca** driver the **libmthca** package is needed.

There is also a known issue relating to connection timeouts in some situations. Refer to Red Hat Bugzilla #470627 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 behavior

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 5.7 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 behavior becomes default in future releases. Users experiencing contention for the malloc resources could try enabling this option.

CHAPTER 4. KNOWN ISSUES

4.1. 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 5.7.

- **Anaconda** does not support XTS encryption for storage volumes. If you have existing XTS encrypted volumes, **Anaconda** will detect them as unpartitioned storage space and ask whether they should be initialized. Make sure to have **Anaconda** ignore any volumes with XTS encryption and configure them for use after installation.

  If you wish to set up new XTS volumes, you will need to do so after installation. Make sure to leave available storage space that you can allocate for the XTS encrypted volumes after installation. (BZ#718123)

- **anaconda** occasionally crashes while attempting to install on a disk containing partitions or file systems used by other operating systems. To workaround this issue, clear the existing partition table using the command:

  ```
  clearpart --initlabel [disks]
  ```

  (BZ#530465)

- Performing a System z installation, when the **`install.img`** is located on direct access storage device (DASD) disk, causes 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

- When installing to an **`ext3`** or **`ext4`** file system, **anaconda** disables periodic file system checking. Unlike **`ext2`**, these file systems are journaled, removing the need for a periodic file system check. In the rare cases where there is an error detected at runtime or an error while recovering the file system journal, the file system check will be run at boot time. (BZ#513480)

- Red Hat Enterprise Linux 5 does not support having a separate **`/var`** on a network file system (**`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 file system. (BZ#485478)

- When using rescue mode on an installation which uses iSCSI drives which were manually configured during installation, the automatic mounting of the root file system does not work. You must configure iSCSI and mount the file systems manually. This only applies to manually 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 file system 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. 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 file system of your installation if wanted

```
$ chroot /mnt/sysimage /bin/su -
```

- 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 file systems, especially the root file system, are directly visible to the host, a host OS reboot may inadvertently parse the partition table and mount the guest file systems. This can lead to highly undesirable outcomes.

- 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.

- 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 adapter 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.

- 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)

- 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 Red Hat Enterprise Linux 5.0 using the updated Virtualized kernel, the upgraded Virtualization RPMs will not match the running kernel. (BZ#251669)

- 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)

- 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)

- 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.

- 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)

- 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)

- When using anaconda's automatic partitioning on an IBM System p partition with multiple hard disks containing different Linux distributions, the anaconda installer may overwrite the

bootloaders of the other Linux installations although their hard disks have been unchecked. To work around this, choose manual partitioning during the installation process.

The following note applies to PowerPC Architectures:

- The minimum RAM required to install Red Hat Enterprise Linux 5.7 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 5.7 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.

The following note applies to s390x Architectures:

- Installation on a machine with existing Linux or non-Linux file systems 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.

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)

4.2. 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)

4.3. 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)

4.4. DEVICE-MAPPER-MULTIPATH

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

- The **/etc/multipath.conf** has a new defaults section parameter: ***file_timeout***. This parameter controls how many seconds **multipathd** will wait for a necessary file to appear while setting up a multipath device. The default is 90 seconds. Note that using the ***file_timeout 0*** parameter will cause mutipathd to crash. (BZ#716329)

- By default, the **multipathd** service starts up before the **iscsi** service. This provides multipathing support early in the bootup process and is necessary for multipathed iSCSI SAN boot setups. However, once started, the **multipathd** service adds paths as informed about them by udev. As soon as the **multipathd** service detects a path that belongs to a multipath device, it creates the device. If the first path that multipathd notices is a passive path, it attempts to make that path active. If it later adds a more optimal path, **multipathd** activates the more optimal path. In some cases, this can cause a significant overhead during a startup.

  If you are experiencing such performance problems, define the **multipathd** service to start after the **iscsi** service. This does not apply to systems where the root device is a multipathed iSCSI device, since it the system would become unbootable. To move the service start time run the following commands:

  ```
  # mv /etc/rc5.d/S06multipathd /etc/rc5.d/S14multipathd
  # mv /etc/rc3.d/S06multipathd /etc/rc3.d/S14multipathd
  ```

  To restore the original start time, run the following command:

  ```
  # chkconfig multipathd resetpriorities
  ```

  (BZ#500998)

- 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)

- 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
```

- 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)

4.5. 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
  ```

- 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”
mkrtootdev –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
```

4.6. 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)

To prevent this from occurring, install the following packages manually:

- librsvg2
- ghostscript-fonts
- pygtk2-libglade

4.7. 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 5.7 for the *IBM System z*does not support the *firstboot* functionality during initial program load.

  To properly initialize setup for Red Hat Enterprise Linux 5.7 on the *IBM System z*, run the following commands after installation:

  - **`/usr/bin/setup`** — provided by the **`setuptool`** package.
  - **`/usr/bin/rhn_register`** — provided by the **`rhn-setup`** package.

  (BZ#217921)

4.8. 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/LogVol00 /
   ```

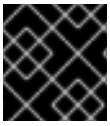
3. Edit the /etc/fstab file from:

   ```
   /dev/VolGroup00/LogVol00 / gfs2 defaults 1 1
   ```

   to

   ```
   /dev/VolGroup00/LogVol00 / gfs2 defaults 1 0
   ```

4. Reboot the system.



IMPORTANT

Note, however that using **GFS2** as the root file system is unsupported.

4.9. 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.

  Alternatively, you can run the following command to mount a device to **/media**:

  ```
  mount /dev/[device name] /media
  ```

4.10. 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)

- Boot-time logging to **/var/log/boot.log** is not available in Red Hat Enterprise Linux 5.7. (BZ#223446, BZ#210136)

4.11. 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)

4.12. KERNEL-XEN

- kernel-xen does not support OProfile on AMD Family 15h processors without any additional settings. Specify the following configuration in the **/etc/modprobe.conf** file in order to enable OProfile:

  ```
  options oprofile timer=1
  ```

  With the above module parameter, the level of OProfile support matches the OProfile support of a bare metal kernel: no hardware performance counter support is available in Red Hat Enterprise Linux 5.7 for AMD Family 15h processors using kernel or kernel-xen. (BZ#720587)

- Red Hat Enterprise Linux 5.7 Xen guests may experience crashes if memory cgroups are used with more than 1 vCPU on a host without the EPT or NPT features. Possible workarounds include:

  1. Run the guest on a HAP (Host Access Protocol) enabled host if the memory cgroups feature is required.

  2. Disable memory cgroups by adding the following option to the guest's kernel command line:

     ```
     cgroup_disable=memory
     ```

  (BZ#700565)

- 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)

- Xen guests will not boot using configurations that bind multiple virtualized CPUs to a single CPU. (BZ#570056)

- 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)

- With certain hardware, **blktap** 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)

- When booting paravirtualized guests that support gigabyte page tables (i.e. a Fedora 11 guest) on Red Hat Enterprise Linux 5.7 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)

- 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

- 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)

- 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 unpause events 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)

The following note applies to x86_64 Architectures:

- Upgrading a host (**dom0**) system to Red Hat Enterprise Linux 5.7 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, BZ#251013)

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/elilo.conf**. (BZ#249076)

- 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)

- 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.

4.13. KERNEL

The kernel packages contain the Linux kernel, the core of any Linux operating system.

- Under some circumstances, error reports within the XFS file system may dereference a NULL pointer and cause kernel panic. (BZ#720551)

- If 32k or more file descriptors are open, a memory leak may occur on a Red Hat Enterprise Linux 5.7 system. (BZ#719495)

- During network installation of Red Hat Enterprise Linux 5.7 on a **tg3** network, networking stops working shortly after the installation process starts. To work around this issue, avoid the network installation for the aforementioned setup, or install Red Hat Enterprise Linux 5.6 and use the **yum update** command to upgrade to Red Hat Enterprise Linux 5.7.

- Changes were made to the **be2net** driver to support multiple receive queues. However, these changes cause the kdump capture kernel to become unresponsive. In order to work around this, the following entry should be added to the **/etc/kdump.conf** file:

  ```
  options be2net multi_rxq=0
  ```

  (BZ#713703)

- On a Red Hat Enterprise Linux 5.7 system, while hand-loading the i386 (32-bit) kernel on z210/z210 SFF with BIOS 1.08, the system may fail to boot. To workaround this issue, please add the following parameter to the boot command line option:

  ```
  pci=nosort
  ```

  (BZ#703538)

- Red Hat Enterprise Linux 5.7 has introduced a new multicast snooping feature for the bridge driver used for virtualization (virt-bridge). This feature is disabled by default in order to not break any existing configurations. To enable this feature, please set the following tunnable parameter to **1**:

  ```
  /sys/class/net/breth0/bridge/multicast_snooping
  ```

  Please note that when multicast snooping is enabled, it may cause a regression with certain switches where it causes a break in the multicast forwarding for some peers.

- By default, **libsas** defines a wideport based on the attached SAS address, rather than the specification compliant “strict” definition of also considering the local SAS address. In Red Hat Enterprise Linux 5.7, only the default “loose” definition is available. The implication is that if an

OEM configures an SCU controller to advertise different SAS addresses per PHY, but hooks up a wide target or an expander to those PHYs, libsas will only create one port. The expectation, in the “strict” case, is that this would result in a single controller multipath configuration.

It is not possible to use a single controller multipath without the **`strict_wide_port`** functionality. Multi-controller multipath should behave as a expected.

A x8 multipath configuration through a single expander can still be obtained under the following conditions:

1. Start with an SCU SKU that exposes (2) x4 controllers (total of 8 PHYs)
2. Assign ***`sas_address1`*** to all the PHYs on **`controller1`**
3. Assign ***`sas_address2`*** to all the PHYs on **`controller2`**
4. Hook up the expander across all 8 PHYs
5. Configure multipath across the two controller instances

It is critical for **`controller1`** to have a distinct address from **`controller2`**, otherwise the expander will be unable to correctly route connection requests to the proper initiator. (BZ#651837)

- On a Red Hat Enterprise Linux 5.7 system, it is advisable to update the firmware of the HP ProLiant Generation 6 (G6) controller's firmware to version 5.02 or later. Once the firmware is successfully updates, reboot the system and kdump will work as expected.

  HP G6 controllers include: P410i, P411, P212, P712, and P812

  In addition, kdump may fail when using the HP Smart Array 5i Controller on a Red Hat Enterprise Linux 5.7 system. (BZ#695493)

- On a Red Hat Enterprise Linux 5.5 and later, suspending the system with the **`lpfc`** driver loaded may crash the system during the resume operation. Therefore, systems using the **`lpfc`** driver, either unload the **`lpfc`** driver before the system is suspended, or ,if that is not possible, do not suspend the system. (BZ#703631)

- NUMA class systems should not be booted with a single memory node configuration. Configuration of single node NUMA systems will result in contention for the memory resources on all of the non-local memory nodes. As only one node will have local memory the CPUs on that single node will starve the remaining CPUs for memory allocations, locks, and any kernel data structure access. This contention will lead to the "CPU#n stuck for 10s!" error messages. This configuration can also result in NMI watchdog timeout panics if a spinlock is acquired via spinlock_irq() and held for more than 60 seconds. The system can also hang for indeterminate lengths of time.

  To minimize this problem, NUMA class systems need to have their memory evenly distributed between nodes. NUMA information can be obtained from dmesg output as well as from the numastat command. (BZ#529428)

- When upgrading from Red Hat Enterprise Linux 5.0, 5.1 or 5.2 to more recent releases, the gfs2-kmod may still be installed on the system. This package must be manually removed or it will override the (newer) version of GFS2 which is built into the kernel. Do not install the **`gfs2-kmod`** package on later versions of Red Hat Enterprise Linux. **`gfs2-kmod`** is not required

since GFS2 is built into the kernel from 5.3 onwards. The content of the gfs2-kmod package is considered a Technology Preview of GFS2, and has not received any updates since Red Hat Enterprise Linux 5.3 was released.

Note that this note only applies to GFS2 and not to GFS, for which the gfs-kmod package continues to be the only method of obtaining the required kernel module.

- Issues might be encountered on a system with 8Gb/s LPe1200x HBAs and firmware version 2.00a3 when the Red Hat Enterprise Linux 5.6 kernel is used with the in-box LPFC driver. Such issues include loss of LUNs and/or fiber channel host hangs during fabric faults with multipathing.

  To work around these issues, it is recommended to either:

  - Downgrade the firmware revision of the 8Gb/s LPe1200x HBA to revision 1.11a5, or
  - Modify the LPFC driver's **`lpfc_enable_npiv`** module parameter to zero.

    When loading the LPFC driver from the initrd image (i.e. at system boot time), add the line

    ```
    options lpfc_enable_npiv=0
    ```

    to **`/etc/modprobe.conf`** and re-build the initrd image.

    When loading the LPFC driver dynamically, include the **`lpfc_enable_npiv=0`** option in the insmod or modprobe command line.

  For additional information on how to set the LPFC driver module parameters, refer to the Emulex Drivers for Linux User Manual.

- If AMD IOMMU is enabled in BIOS on ProLiant DL165 G7 systems, the system will reboot automatically when IOMMU attempts to initialize. To work around this issue, either disable IOMMU, or update the BIOS to version **`2010.09.06`** or later. (BZ#628534)

- As of Red Hat Enterprise Linux 5.6 the **`ext4`** file system is fully supported. However, provisioning ext4 file systems with the anaconda installer is not supported, and ext4 file systems need to be provisioned manually after the installation. (BZ#563943)

- In some cases the NFS server fails to notify NFSv4 clients about renames and unlinks done by other clients, or by non-NFS users of the server. An application on a client may then be able to open the file at its old pathname (and read old cached data from it, and perform read locks on it), long after the file no longer exists at that pathname on the server.

  To work around this issue, use NFSv3 instead of NFSv4. Alternatively, turn off support for leases by writing ***`0`*** to **`/proc/sys/fs/leases-enable`** (ideally on boot, before the nfs server is started). This change prevents NFSv4 delegations from being given out, restore correctness at the expense of some performance.

- Some laptops may generate continuous events in response to the lid being shut. Consequently, the gnome-power-manager utility will consume CPU resources as it responds to each event. (BZ#660644)

- 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)

- 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)

- Memory on-line is not currently supported with the Boxboro-EX platform. (BZ#515299)

- 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)

- Data corruption on NFS file systems 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

- 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 partition (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)

- 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)

- 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)

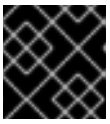
- The kernel is unable to properly detect whether there is media present in a CD-ROM drive during kickstart installs. The function to check the presence of media incorrectly interprets the "logical unit is becoming ready" sense, returning that the drive is ready when it is not. To work around this issue, wait several seconds between inserting a CD and asking the installer (anaconda) to refresh the CD. (BZ#510632)

- 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)

- 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 file system like **`tmpfs`** or **`ramfs`** is mounted.

  To work around this issue, unmount all RAM based file systems (i.e. tmpfs or ramfs). If unmounting the RAM based file systems 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)

- Configuring IRQ SMP affinity has no effect on some devices that use message signaled 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=nomsi**. (BZ#432451)

- The **smartctl** tool cannot properly read SMART parameters from SATA devices. (BZ#429606)

- *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)

- 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)

- 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)

- 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)

- 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)

- 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)

- 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)

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)

4.14. 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)
- 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)
- **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)
- 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)
- 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)

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)

4.15. 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).

- Booting a Linux guest causes 1.5 to 2 second time drift from the host time when the default hwclock service starts. It is recommended to disable the hwclock service. Alternatively, enable the ntp service so ntp can correct the time once the ntp service starts. (BZ#523478)

- By default, KVM virtual machines created in Red Hat Enterprise Linux 5.6 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
```

- 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 file system, 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.

- 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)

- The use of the qcow2 disk image format with KVM is considered a Technology Preview. (BZ#517880)

- 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)

- Hot plugging emulated devices after migration may result in the virtual machine crashing after a reboot or the devices no longer being visible. (BZ#507191)

- The KVM modules from the **kmod-kvm** package do not support kernels prior to version 2.6.18-203.el5. If kmod-kvm is updated and an older kernel is kept installed, error messages similar to the following will be returned if attempting to install these modules on older kernels:

```
WARNING: /lib/modules/2.6.18-194.el5/weak-updates/kmod-kvm/ksm.ko
needs unknown symbol kvm_ksm_spte_count
```

(BZ#509361)

- 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)

- 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)).

- The following QEMU / KVM features are currently disabled and not supported: (BZ#512837)
  - 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 and es1370 sound card emulations
  - bluetooth emulation

4.16. 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)

4.17. 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)

- 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)

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 file system during the first boot. (BZ#529636)

4.18. 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)

4.19. 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)

- 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)

- 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)

4.20. PERL-LIBXML-ENNO

The perl-libxml-enno modules were used for XML parsing and validation.

- Note: the perl-libxml-enno library did not ship in any Red Hat Enterprise Linux 5 release. (BZ#612589)

4.21. PM-UTILS

The pm-utils package contains utilities and scripts for power management.

- nVidia video devices on laptops can not be correctly re-initialized using VESA in Red Hat Enterprise Linux 5. Attempting to do so results in a black laptop screen after resume from suspend.

4.22. RPM

The RPM Package Manager (RPM) is a command line driven package management system capable of installing, uninstalling, verifying, querying, and updating software packages.

- Users of a freshly-installed PowerPC Red Hat Enterprise Linux 5.8 system may encounter package-related operation failures with the following errors:

  ```
  rpmdb: PANIC: fatal region error detected; run recovery
  error: db4 error(-30977) from db->sync: DB_RUNRECOVERY: Fatal error,
  run
  database recovery
  ```

4.23. 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.

4.24. SSSD

The System Security Services Daemon (SSSD) provides a set of daemons to manage access to remote directories and authentication mechanisms. It provides an NSS and PAM interface toward the system and a pluggable back-end system to connect to multiple different account sources. It is also the basis to provide client auditing and policy services for projects such as FreeIPA.

- When SSSD communicates with an OpenLDAP server, which supports server-side password policies but does not list them in the ***`supportedControl`*** attribute of the server's rootDSE entry, SSSD terminates unexpectedly with a segmentation fault. (BZ#713961)

4.25. 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 evens 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)

- 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)

4.26. VDSM22

- If an ISO domain includes a CD-ROM image that uses spaces or other special shell characters, a virtual machine that is configured to boot with the image attached will fail to start. To avoid this, use only alphanumeric names for image names.

4.27. 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.

- 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.

4.28. 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)

- 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)

4.29. 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)

- 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)

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, BZ#221789)

4.30. 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 highers than 800x600.

  To work around this, add the following line to the **ServerLayout** section of **/etc/X11/xorg.conf**:

  ```
  Option "Int10Backend" "x86emu"
  ```

  (BZ#236416)

4.31. 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)

4.32. XEN

- There are only 2 virtual slots (00:06.0 and 00:07.0) that are available for hot plug support in a virtual guest. (BZ#564261)

- 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 behavior is required, disable pci-dev-assign-strict-check in /etc/xen/xend-config.sxp. (BZ#508310)

- 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)

- 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)

- 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, BZ#429154)

- 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)

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)

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. CLIENT

A.1.1. Added Packages

buildsys-macros-5-5.el5

- Group: Development/System
- Summary: Build system macros
- Description: Build system macros

cmake-2.6.4-5.el5.4

- Group: Development/Tools
- Summary: Cross-platform make system
- Description: CMake is used to control the software compilation process using simple platform and compiler independent configuration files. CMake generates native makefiles and workspaces that can be used in the compiler environment of your choice. CMake is quite sophisticated: it is possible to support complex environments requiring system configuration, preprocessor generation, code generation, and template instantiation.

ding-libs-0.1.2-10.el5

- Group: Development/Libraries
- Summary: "Ding is not GLib" assorted utility libraries
- Description: A set of helpful libraries used by projects such as SSSD.

jline-0.9.94-0.9.el5_6

- Group: Development/Libraries
- Summary: Java library for reading and editing user input in console applications
- Description: JLine is a java library for reading and editing user input in console applications. It features tab-completion, command history, password masking, customizable keybindings, and pass-through handlers to use to chain to other console applications.

libcxgb4-1.1.1-2.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.

man-pages-overrides-0.5.7.3-3.el5

- Group: Documentation
- Summary: Complementary and updated manual pages
- Description: A collection of manual ("man") pages to complement other packages or update those contained therein. Always have the latest version of this package installed.

openldap24-libs-2.4.23-5.el5

- Group: System Environment/Daemons
- Summary: LDAP support libraries
- 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.

openscap-0.7.2-1.el5

- Group: System Environment/Libraries
- Summary: Set of open source libraries enabling integration of the SCAP line of standards
- Description: OpenSCAP is a set of open source libraries providing an easier path for integration of the SCAP line of standards. SCAP is a line of standards managed by NIST with the goal of providing a standard language for the expression of Computer Network Defense related information.

perl-NetAddr-IP-4.027-5.el5

- Group: Development/Libraries
- Summary: Manages IPv4 and IPv6 addresses and subnets
- Description: This module provides an object-oriented abstraction on top of IP addresses or IP subnets, that allows for easy manipulations. Version 4.xx of NetAdder::IP will will work older versions of Perl and does not use Math::BigInt as in previous versions.

python-ethtool-0.6-5.el5

- Group: System Environment/Libraries
- Summary: Ethernet settings python bindings
- Description: Python bindings for the ethtool kernel interface, that allows querying and changing of Ethernet card settings, such as speed, port, auto-negotiation, and PCI locations.

python-rhsm-0.95.5.5-1.el5

- Group: Development/Libraries
- Summary: A Python library to communicate with a Red Hat Unified Entitlement Platform

- Description: A small library for communicating with the REST interface of a Red Hat Unified Entitlement Platform. This interface is used for the management of system entitlements, certificates, and access to content.

python-simplejson-2.0.9-8.el5

- Group: System Environment/Libraries
- Summary: Simple, fast, extensible JSON encoder/decoder for Python
- Description: simplejson is a simple, fast, complete, correct and extensible JSON <http://json.org> encoder and decoder for Python 2.4+. It has no external dependencies. simplejson was formerly known as simple_json, but changed its name to comply with PEP 8 module naming guidelines. The encoder may be subclassed to provide serialization in any kind of situation, without any special support by the objects to be serialized (somewhat like pickle). The decoder can handle incoming JSON strings of any specified encoding (UTF-8 by default).

python-suds-0.4.1-2.el5

- Group: Development/Libraries
- Summary: A python SOAP client
- Description: The suds project is a python soap web services client lib. Suds leverages python meta programming to provide an intuitive API for consuming web services. Objectification of types defined in the WSDL is provided without class generation. Programmers rarely need to read the WSDL since services and WSDL based objects can be easily inspected.

rhino-1.7-0.7.r2.3.el5_6

- Group: Development/Libraries/Java
- Summary: JavaScript for Java
- Description: Rhino is an open-source implementation of JavaScript written entirely in Java. It is typically embedded into Java applications to provide scripting to end users.

subscription-manager-0.95.5.21-1.el5

- Group: System Environment/Base
- Summary: Tools and libraries for subscription and repository management
- Description: The Subscription Manager package provides programs and libraries to allow users to manage subscriptions and yum repositories from the Red Hat entitlement platform.

tcsh617-6.17-5.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.

virt-what-1.11-2.el5

- Group: Applications/Emulators
- Summary: Detect if we are running in a virtual machine
- Description: virt-what is a shell script which can be used to detect if the program is running in a virtual machine. The program prints out a list of "facts" about the virtual machine, derived from heuristics. One fact is printed per line. If nothing is printed and the script exits with code 0 (no error), then it can mean either that the program is running on bare-metal or the program is running inside a type of virtual machine which we don't know about or cannot detect. Current types of virtualization detected:
  - hyperv - Microsoft Hyper-V
  - kvm - Linux Kernel Virtual Machine (KVM)
  - openvz - OpenVZ or Virtuozzo
  - powervm_lx86 - IBM PowerVM Lx86 Linux/x86 emulator
  - qemu - QEMU (unaccelerated)
  - uml - User-Mode Linux (UML)
  - virtage - Hitachi Virtualization Manager (HVM) Virtage LPAR
  - virtualbox - VirtualBox
  - virtualpc - Microsoft VirtualPC
  - vmware - VMware
  - xen - Xen
  - xen-dom0 - Xen dom0 (privileged domain)
  - xen-domU - Xen domU (paravirtualized guest domain)
  - xen-hvm - Xen guest fully virtualized (HVM)

A.1.2. Dropped Packages

None

A.1.3. Updated Packages

NetworkManager-0.7.0-10.el5_5.2 - NetworkManager-0.7.0-13.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

SysVinit-2.86-15.el5 - SysVinit-2.86-17.el5

- Group: System Environment/Base
- Summary: Programs which control basic system processes.
- Description: The SysVinit package contains a group of processes that control the very basic functions of your system. SysVinit includes the init program, the first program started by the Linux kernel when the system boots. Init then controls the startup, running, and shutdown of all other 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

anaconda-11.1.2.224-1 - anaconda-11.1.2.242-1

- 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.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

apr-1.2.7-11.el5_5.3 - apr-1.2.7-11.el5_6.5

- Group: System Environment/Libraries
- Summary: Apache Portable Runtime library
- Description: The mission of the Apache Portable Runtime (APR) is to provide a free library of C data structures and routines, forming a system portability layer to as many operating systems as possible, including Unices, MS Win32, BeOS and OS/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

authconfig-5.3.21-6.el5 - authconfig-5.3.21-7.el5

- Group: System Environment/Base
- Summary: Command line tool for setting up authentication from network services
- Description: Authconfig is a command line utility which can configure a workstation to use shadow (more secure) passwords. Authconfig can also configure a system to be a client for certain networked user information and authentication schemes.
- 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.rc2.143.el5_5.6 - autofs-5.0.1-0.rc2.156.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

avahi-0.6.16-9.el5_5 - avahi-0.6.16-10.el5_6

- 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

bash-3.2-24.el5 - bash-3.2-32.el5

- Group: System Environment/Shells
- Summary: The GNU Bourne Again shell (bash) version 3.2
- Description: The GNU Bourne Again shell (Bash) is a shell or command language interpreter that is compatible with the Bourne shell (sh). Bash incorporates useful features from the Korn shell (ksh) and the C shell (csh). Most sh scripts can be run by bash without modification. This package (bash) contains bash version 3.2, which improves POSIX compliance over previous versions.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

bind97-9.7.0-6.P2.el5 - bind97-9.7.0-6.P2.el5_6.3

- 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

booty-0.80.6-7 - booty-0.80.6-10

- 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

bridge-utils-1.1-2 - bridge-utils-1.1-3.el5

- Group: System Environment/Base
- Summary: Utilities for configuring the linux ethernet bridge
- Description: This package contains utilities for configuring the linux ethernet bridge. The linux ethernet bridge can be used for connecting multiple ethernet devices together. The connecting is fully transparent: hosts connected to one ethernet device see hosts connected to the other ethernet devices directly. Install bridge-utils if you want to use the linux ethernet bridge.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

busybox-1.2.0-7.el5 - busybox-1.2.0-10.el5

- Group: System Environment/Shells

- Summary: Statically linked binary providing simplified versions of system commands
- Description: Busybox is a single binary which includes versions of a large number of system commands, including a shell. This package can be very useful for recovering from certain types of system failures, particularly those involving broken shared libraries.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

certmonger-0.30-4.el5 - certmonger-0.42-1.el5

- Group: System Environment/Daemons
- Summary: Certificate status monitor and PKI enrollment client
- Description: Certmonger is a service which is primarily concerned with getting your system enrolled with a certificate authority (CA) and keeping it enrolled.
- Added Dependencies:
  - e2fsprogs-devel
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cman-2.0.115-68.el5 - cman-2.0.115-85.el5

- Group: System Environment/Base
- Summary: cman - The Cluster Manager
- Description: cman - The Cluster Manager

- Added Dependencies:
  - libxslt
  - pexpect
  - python-pycurl
  - python-suds
- 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_4.2 - coreutils-5.97-34.el5

- 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

cpuspeed-1.2.1-9.el5 - cpuspeed-1.2.1-10.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

cryptsetup-luks-1.0.3-5.el5 - cryptsetup-luks-1.0.3-8.el5

- Group: Applications/System
- Summary: A utility for setting up encrypted filesystems
- Description: This package contains cryptsetup, a utility for setting up encrypted filesystems using Device Mapper and the dm-crypt target.
- 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-1.3.7-26.el5 - cups-1.3.7-26.el5_6.1

- 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.
- No added dependencies
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

curl-7.15.5-9.el5 - curl-7.15.5-9.el5_6.3

- 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_4.3 - cyrus-imapd-2.3.7-12.el5

- 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
- Removed Dependencies:
  - lm_sensors-devel
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dapl-2.0.25-2.el5_5.1 - dapl-2.0.25-2.el5_6.1

- 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.
- 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-1.1.2-14.el5 - dbus-1.1.2-15.el5_6

- 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

dejagnu-1.4.4-5.1 - dejagnu-1.4.4-7.el5

- Group: Development/Tools
- Summary: A front end for testing other programs.
- Description: DejaGnu is an Expect/Tcl based framework for testing other programs. DejaGnu has several purposes: to make it easy to write tests for any program; to allow you to write tests which will be portable to any host or target where a program must be tested; and to standardize the output format of all tests (making it easier to integrate the testing into software development).
- 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-1.02.55-2.el5 - device-mapper-1.02.63-4.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-0.4.7-42.el5 - device-mapper-multipath-0.4.7-46.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-3.0.5-23.el5_5.2 - dhcp-3.0.5-29.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

dmidecode-2.10-3.el5 - dmidecode-2.11-1.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.rc13-63.el5 - dmraid-1.0.0.rc13-65.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

dogtail-0.6.1-3.el5 - dogtail-0.6.1-4.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

e2fsprogs-1.39-23.el5_5.1 - e2fsprogs-1.39-33.el5

- Group: System Environment/Base
- Summary: Utilities for managing the second and third extended (ext2/ext3) filesystems
- Description: The e2fsprogs package contains a number of utilities for creating, checking, modifying, and correcting any inconsistencies in second and third extended (ext2/ext3) filesystems. E2fsprogs contains e2fsck (used to repair filesystem inconsistencies after an unclean shutdown), mke2fs (used to initialize a partition to contain an empty ext2 filesystem), debugfs (used to examine the internal structure of a filesystem, to manually repair a corrupted filesystem, or to create test cases for e2fsck), tune2fs (used to modify filesystem parameters), and most of the other core ext2fs filesystem utilities. You should install the e2fsprogs package if you need to manage the performance of an ext2 and/or ext3 filesystem.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

emacs-21.4-20.el5 - emacs-21.4-24.el5

- Group: Applications/Editors
- Summary: GNU Emacs text editor
- Description: Emacs is a powerful, customizable, self-documenting, modeless text editor. Emacs contains special code editing features, a scripting language (elisp), and the capability to read mail, news, and more without leaving the editor. This package provides an emacs binary with support for X windows.
- 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-5.4.4-13.el5 - etherboot-5.4.4-15.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
- 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-4.63-5.el5_5.2 - exim-4.63-10.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

finger-0.17-32.2.1.1 - finger-0.17-33

- Group: Applications/Internet
- Summary: The finger client.
- Description: Finger is a utility which allows users to see information about system users (login name, home directory, name, how long they've been logged in to the system, etc.). The finger package includes a standard finger client. You should install finger if you'd like to retrieve finger information from other 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

firefox-3.6.13-2.el5 - firefox-3.6.18-1.el5_6

- 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 >= 1.9.2.18-1
- Removed Dependencies:
  - xulrunner-devel >= 1.9.2.13-3
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

fonts-indic-2.3.1-1.el5 - fonts-indic-2.3.1.1-2.el5

- Group: User Interface/X
- Summary: Free Indian truetype/opentype fonts
- Description: This package provides the Hindi, Bengali, Gujarati, Punjabi, Tamil, Kannada,\ Malayalam, Oriya, Telugu TrueType/Opentype fonts.
- 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-4.1.2-50.el5 - gcc-4.1.2-51.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

gdb-7.0.1-32.el5 - gdb-7.0.1-37.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.
- 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-0.1.62-28.el5 - gfs2-utils-0.1.62-31.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

giflib-4.1.3-7.1.el5_3.1 - giflib-4.1.3-7.3.3.el5

- Group: System Environment/Libraries
- Summary: Library for manipulating GIF format image files
- Description: The giflib package contains a shared library of functions for loading and saving GIF format image files. It is API and ABI compatible with libungif, the library which supported uncompressed GIFs while the Unisys LZW patent was in effect. Install the giflib package if you need to write programs that use GIF files. You should also install the giflib-utils package if you need some simple utilities to manipulate GIFs.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gimp-2.2.13-2.0.7.el5 - gimp-2.2.13-2.0.7.el5_6.2

- Group: Applications/Multimedia
- Summary: GNU Image Manipulation Program
- Description: GIMP (GNU Image Manipulation Program) is a powerful image composition and editing program, which can be extremely useful for creating logos and other graphics for webpages. GIMP has many of the tools and filters you would expect to find in similar commercial offerings, and some interesting extras as well. GIMP provides a large image manipulation toolbox, including channel operations and layers, effects, sub-pixel imaging and anti-aliasing, and conversions, all with multi-level undo.
- 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-2.5-58 - glibc-2.5-65

- 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-screensaver-2.16.1-8.el5_5.2 - gnome-screensaver-2.16.1-8.el5_6.3

- Group: Amusements/Graphics
- Summary: GNOME Screensaver
- Description: gnome-screensaver is a screen saver and locker that aims to have simple, sane, secure defaults and be well integrated with the desktop.
- 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-terminal-2.16.0-5.3.el5 - gnome-terminal-2.16.0-5.3.el5_6.1

- Group: User Interface/Desktops
- Summary: GNOME Terminal
- Description: GNOME terminal emulator application.
- 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-vfs2-2.16.2-6.el5_5.1 - gnome-vfs2-2.16.2-8.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.
- 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-1.3.5-11.el5_4.1 - gzip-1.3.5-13.el5

- 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

hplip-1.6.7-6.el5 - hplip-1.6.7-6.el5_6.1

- Group: System Environment/Daemons
- Summary: HP Linux Imaging and Printing Project
- Description: The Hewlett-Packard Linux Imaging and Printing Project provides drivers for HP printers and multi-function peripherals.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

hplip3-3.9.8-11.el5 - hplip3-3.9.8-11.el5_6.1

- Group: System Environment/Daemons
- Summary: HP Linux Imaging and Printing Project

- Description: The Hewlett-Packard Linux Imaging and Printing Project provides drivers for HP printers and multi-function peripherals.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

httpd-2.2.3-45.el5 - httpd-2.2.3-53.el5

- Group: System Environment/Daemons
- Summary: Apache HTTP Server
- Description: The Apache HTTP Server is a powerful, efficient, and extensible web 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

hwdata-0.213.22-1.el5 - hwdata-0.213.24-1.el5

- 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

initscripts-8.45.33-1.el5 - initscripts-8.45.38-2.el5

- Group: System Environment/Base
- Summary: The inittab file and the /etc/init.d scripts.
- Description: The initscripts package contains the basic system scripts used to boot your Red Hat system, change runlevels, and shut the system down cleanly. Initscripts also contains the scripts that activate and deactivate most network interfaces.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ipa-client-2.0-10.el5 - ipa-client-2.0-14.el5

- Group: System Environment/Base
- Summary: IPA authentication for use on clients
- Description: IPA is an integrated solution to provide centrally managed Identity (machine, user, virtual machines, groups, authentication credentials), Policy (configuration settings, access control information) and Audit (events, logs, analysis thereof).
- Added Dependencies:
  - authconfig
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

iscsi-initiator-utils-6.2.0.872-6.el5 - iscsi-initiator-utils-6.2.0.872-10.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
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

java-1.6.0-openjdk-1.6.0.0-1.16.b17.el5 - java-1.6.0-openjdk-1.6.0.0-1.22.1.9.8.el5_6

- Group: Development/Languages
- Summary: OpenJDK Runtime Environment
- Description: The OpenJDK runtime environment.
- Added Dependencies:
  - ant-nodeps
  - redhat-lsb
  - rhino
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

jwhois-3.2.3-11.el5 - jwhois-3.2.3-12.el5

- Group: Applications/Internet
- Summary: Internet whois/nicname client.
- Description: A whois client that accepts both traditional and finger-style queries.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

kdebase-3.5.4-22.el5 - kdebase-3.5.4-24.el5

- Group: User Interface/Desktops
- Summary: K Desktop Environment - core files
- Description: Core applications for the K Desktop Environment. Included are: kdm (replacement for xdm), kwin (window manager), konqueror (filemanager, web browser, ftp client, ...), konsole (xterm replacement), kpanel (application starter and desktop pager), kaudio (audio server), kdehelp (viewer for kde help files, info and man pages), kthememgr (system for managing alternate theme packages) plus other KDE components (kcheckpass, kikbd, kscreensaver, kcontrol, kfind, kfontmanager, kmenuedit).
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

kdenetwork-3.5.4-9.el5 - kdenetwork-3.5.4-13.el5_6.1

- Group: Applications/Internet
- Summary: K Desktop Environment - Network Applications
- Description: Networking applications for the K Desktop 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

kernel-2.6.18-238.el5 - kernel-2.6.18-274.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-126.el5 - kexec-tools-1.102pre-126.el5_6.6

- Group: Applications/System
- Summary: The kexec/kdump userspace component.
- 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

krb5-1.6.1-55.el5 - krb5-1.6.1-62.el5

- 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-20100202-1.el5_5.1 - ksh-20100202-1.el5_6.6

- 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

kvm-83-224.el5 - kvm-83-239.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-debug-devel = 2.6.18-269.el5
  - kernel-devel = 2.6.18-269.el5
- Removed Dependencies:
  - kernel-debug-devel = 2.6.18-237.el5
  - kernel-devel = 2.6.18-237.el5
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

lapack-3.0-37.el5 - lapack-3.0-38.el5

- Group: Development/Libraries
- Summary: The LAPACK libraries for numerical linear algebra
- Description: LAPACK (Linear Algebra PACKage) is a standard library for numerical linear algebra. LAPACK provides routines for solving systems of simultaneous linear equations, least-squares solutions of linear systems of equations, eigenvalue problems, and singular value problems. Associated matrix factorizations (LU, Cholesky, QR, SVD, Schur, and generalized Schur) and related computations (i.e., reordering of Schur factorizations and

estimating condition numbers) are also included. LAPACK can handle dense and banded matrices, but not general sparse matrices. Similar functionality is provided for real and complex matrices in both single and double precision. LAPACK is coded in Fortran77 and built with gcc.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libdhcp-1.20-10.el5 - libdhcp-1.20-11.el5

- Group: Development/Libraries
- Summary: A library for network interface configuration with DHCP
- Description: libdhcp enables programs to invoke and control the Dynamic Host Configuration Protocol (DHCP) clients: the Internet Software Consortium (ISC) IPv4 DHCP client library, libdhcp4client, and the IPv6 DHCPv6 client library, libdhcp6client, and provides Network Interface Configuration (NIC) services for network parameter autoconfiguration with DHCP.
- Added Dependencies:
  - dhcp-devel >= 12:3.0.5-26
  - libdhcp4client-devel >= 12:3.0.5-26
- Removed Dependencies:
  - dhcp-devel >= 12:3.0.5-13
  - libdhcp4client-devel >= 12:3.0.5-13
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libmlx4-1.0.1-5.el5 - libmlx4-1.0.1-6.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.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libtdb-1.2.1-5.el5 - libtdb-1.2.1-6.el5

- Group: System Environment/Daemons
- Summary: The tdb library
- Description: A library that implements a trivial database.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libtiff-3.8.2-7.el5_5.5 - libtiff-3.8.2-7.el5_6.7

- Group: System Environment/Libraries
- Summary: Library of functions for manipulating TIFF format image files
- Description: The libtiff package contains a library of functions for manipulating TIFF (Tagged Image File Format) image format files. TIFF is a widely used file format for bitmapped images. TIFF files usually end in the .tif extension and they are often quite large.

The libtiff package should be installed if you need to manipulate TIFF format image 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

libuser-0.54.7-2.1.el5_4.1 - libuser-0.54.7-2.1.el5_5.2

- 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:
  - openldap-clients
  - openldap-servers
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libvirt-0.8.2-15.el5 - libvirt-0.8.2-22.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

libxml2-2.6.26-2.1.2.8.el5_5.1 - libxml2-2.6.26-2.1.12

- Group: Development/Libraries
- Summary: Library providing XML and HTML support
- Description: This library allows to manipulate XML files. It includes support to read, modify and write XML and HTML files. There is DTDs support this includes parsing and validation even with complex DtDs, either at parse time or later once the document has been modified. The output can be a simple SAX stream or and in-memory DOM like representations. In this case one can use the built-in XPath and XPointer implementation to select subnodes or ranges. A flexible Input/Output mechanism is available, with existing HTTP and FTP modules and combined to an URI 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

linuxwacom-0.7.8.3-10.el5 - linuxwacom-0.7.8.3-11.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

logrotate-3.7.4-9.el5_5.2 - logrotate-3.7.4-12

- Group: System Environment/Base
- Summary: Rotates, compresses, removes and mails system log files.
- Description: The logrotate utility is designed to simplify the administration of log files on a system which generates a lot of log files. Logrotate allows for the automatic rotation compression, removal and mailing of log files. Logrotate can be set to handle a log file daily, weekly, monthly or when the log file gets to a certain size. Normally, logrotate runs as a daily cron job. Install the logrotate package if you need a utility to deal with the log files on your 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

logwatch-7.3-8.el5 - logwatch-7.3-9.el5_6

- 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

lvm2-2.02.74-5.el5 - lvm2-2.02.84-6.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.
- Added Dependencies:
  - device-mapper >= 1.02.63-2
- Removed Dependencies:
  - device-mapper >= 1.02.55-2
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

m2crypto-0.16-6.el5.8 - m2crypto-0.16-8.el5

- Group: System Environment/Libraries
- Summary: Support for using OpenSSL in python scripts
- Description: This package allows you to call OpenSSL functions from python scripts.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mailman-2.1.9-6.el5 - mailman-2.1.9-6.el5_6.1

- Group: Applications/Internet
- Summary: Mailing list manager with built in Web access.
- Description: Mailman is software to help manage email discussion lists, much like Majordomo and Smartmail. Unlike most similar products, Mailman gives each mailing list a webpage, and allows users to subscribe, unsubscribe, etc. over the Web. Even the list manager can administer his or her list entirely from the Web. Mailman also integrates most things people want to do with mailing lists, including archiving, mail <-> news gateways, and so on.

  Documentation can be found in: /usr/share/doc/mailman-2.1.9

  When the package has finished installing, you will need to perform some additional installation steps, these are described in: /usr/share/doc/mailman-2.1.9/INSTALL.REDHAT
- 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-1.6d-1.1 - man-1.6d-2.el5

- Group: System Environment/Base
- Summary: A set of documentation tools: man, apropos and whatis.
- Description: The man package includes three tools for finding information and/or documentation about your Linux system: man, apropos, and whatis. The man system formats and displays on-line manual pages about commands or functions on your system. Apropos searches the whatis database (containing short descriptions of system commands) for a string. Whatis searches its own database for a complete word. The man package should be installed on your system because it is the primary way to find documentation on a Linux 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

mcelog-0.9pre-1.29.el5 - mcelog-0.9pre-1.32.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
- No added obsoletes
- No removed obsoletes

mkinitrd-5.1.19.6-68.el5 - mkinitrd-5.1.19.6-71.el5

- 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

mod_authz_ldap-0.26-9.el5_5.1 - mod_authz_ldap-0.26-11.el5

- Group: System Environment/Daemons
- Summary: LDAP authorization module for the Apache HTTP Server
- Description: The mod_authz_ldap package provides support for authenticating users of the Apache HTTP server against an LDAP database. mod_authz_ldap features the ability to authenticate users based on the SSL client certificate presented, and also supports password aging, and authentication based on role or by configured filters.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mod_nss-1.0.8-3.el5 - mod_nss-1.0.8-4.el5_6.1

- Group: System Environment/Daemons
- Summary: SSL/TLS module for the Apache HTTP server
- Description: The mod_nss module provides strong cryptography for the Apache Web server via the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols using the Network Security Services (NSS) security 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

mysql-5.0.77-4.el5_5.4 - mysql-5.0.77-4.el5_6.6

- 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-2.16.2-7.el5 - nautilus-2.16.2-10.el5

- Group: User Interface/Desktops
- Summary: Nautilus is a file manager for GNOME.
- Description: Nautilus integrates access to files, applications, media, Internet-based resources and the Web. Nautilus delivers a dynamic and rich user experience. Nautilus is an free software project developed under the GNU General Public License and is a core component of the GNOME desktop 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

net-snmp-5.3.2.2-9.el5_5.1 - net-snmp-5.3.2.2-14.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

nfs-utils-1.0.9-50.el5 - nfs-utils-1.0.9-54.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
- No removed obsoletes

nss-3.12.8-1.el5 - nss-3.12.8-4.el5_6

- Group: System Environment/Libraries
- Summary: Network Security Services
- Description: Network Security Services (NSS) is a set of libraries designed to support cross-platform development of security-enabled client and server applications. Applications built with NSS can support SSL v2 and v3, TLS, PKCS #5, PKCS #7, PKCS #11, PKCS #12, S/MIME, X.509 v3 certificates, and other security standards.
- 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-253-37.el5 - nss_ldap-253-42.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:
  - openssl-devel >= 0.9.8e-18
- Removed Dependencies:
  - openssl-devel

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ntp-4.2.2p1-9.el5_4.1 - ntp-4.2.2p1-15.el5

- 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-0.9.8-11.el5 - numactl-0.9.8-12.el5_6

- 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

openais-0.80.6-28.el5 - openais-0.80.6-30.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-1.4.1-5.el5 - openib-1.4.1-6.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-2.3.43-12.el5_5.3 - openldap-2.3.43-12.el5_6.7

- 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

openoffice.org-3.1.1-19.5.el5_5.1 - openoffice.org-3.1.1-19.5.el5_5.6

- 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.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

opensm-3.3.3-1.el5 - opensm-3.3.3-2.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.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openssh-4.3p2-72.el5 - openssh-4.3p2-72.el5_6.3

- 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_5.7 - openssl-0.9.8e-20.el5

- 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_5.3 - openswan-2.6.21-5.el5_6.4

- 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

pam_krb5-2.2.14-18.el5 - pam_krb5-2.2.14-21.el5

- 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

pango-1.14.9-8.el5 - pango-1.14.9-8.el5_6.2

- Group: System Environment/Libraries
- Summary: System for layout and rendering of internationalized text
- Description: Pango is a system for layout and rendering of internationalized text.
- 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-0.6.6-19.el5 - paps-0.6.6-20.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-1.8.1-27.el5 - parted-1.8.1-28.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

pcre-6.6-6.el5 - pcre-6.6-6.el5_6.1

- Group: System Environment/Libraries
- Summary: Perl-compatible regular expression library
- Description: Perl-compatible regular expression library. PCRE has its own native API, but a set of "wrapper" functions that are based on the POSIX API are also supplied in the library libpcreposix. Note that this just provides a POSIX calling interface to PCRE: the regular expressions themselves still follow Perl syntax and semantics. The header file for the POSIX-style functions is called pcreposix.h.
- 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-5.8.8-32.el5_5.2 - perl-5.8.8-32.el5_6.3

- Group: Development/Languages
- Summary: The Perl programming language
- Description: Perl is a high-level programming language with roots in C, sed, awk and shell scripting. Perl is good at handling processes and files, and is especially good at handling text. Perl's hallmarks are practicality and efficiency. While it is used to do a lot of different things, Perl's most common applications are system administration utilities and web programming. A large proportion of the CGI scripts on the web are written in Perl. You need the perl package installed on your system so that your system can handle Perl scripts. Install this package if you want to program in Perl or enable your system to handle Perl scripts.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

php53-5.3.3-1.el5 - php53-5.3.3-1.el5_6.1

- Group: Development/Languages
- Summary: PHP scripting language for creating dynamic web sites
- 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

poppler-0.5.4-4.4.el5_5.14 - poppler-0.5.4-4.4.el5_6.17

- 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

postfix-2.3.3-2.1.el5_2 - postfix-2.3.3-2.3.el5_6

- Group: System Environment/Daemons
- Summary: Postfix Mail Transport Agent
- Description: Postfix is a Mail Transport Agent (MTA), supporting LDAP, SMTP AUTH (SASL), TLS
- 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-8.1.22-1.el5_5.1 - postgresql-8.1.23-1.el5_6.1

- 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

postgresql84-8.4.5-1.el5_5.1 - postgresql84-8.4.7-1.el5_6.1

- 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.

- 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-3.2.7-16.el5 - procps-3.2.7-17.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 pdwx. 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

psmisc-22.2-7 - psmisc-22.2-7.el5_6.2

- Group: Applications/System
- Summary: Utilities for managing processes on your system.
- Description: The psmisc package contains utilities for managing processes on your system: pstree, killall and fuser. The pstree command displays a tree structure of all of the running processes on your system. The killall command sends a specified signal (SIGTERM if nothing is specified) to processes identified by name. The fuser command identifies the PIDs of processes that are using specified files or 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

pyOpenSSL-0.6-1.p24.7.2.2 - pyOpenSSL-0.6-2.el5

- Group: Development/Libraries
- Summary: Python wrapper module around the OpenSSL library
- Description: High-level wrapper around a subset of the OpenSSL library, includes * SSL.Connection objects, wrapping the methods of Python's portable sockets * Callbacks written in Python * Extensive error-handling mechanism, mirroring OpenSSL's error codes ... and much more ;)
- 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-0.43.8-1.el5 - pykickstart-0.43.9-1.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-2.4.3-43.el5 - python-2.4.3-44.el5

- Group: Development/Languages
- Summary: An interpreted, interactive, object-oriented programming language.
- Description: Python is an interpreted, interactive, object-oriented programming language often compared to Tcl, Perl, Scheme or Java. Python includes modules, classes, exceptions, very high level dynamic data types and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems (X11, Motif, Tk, Mac and MFC). Programmers can write new built-in modules for Python in C or C++. Python can be used as an extension language for applications that need a programmable interface. This package contains most of the standard Python modules, as well as modules for interfacing to the Tix widget set for Tk and RPM. Note that documentation for Python is provided in the python-docs 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

python-imaging-1.1.5-5.el5 - python-imaging-1.1.5-7.el5

- Group: Development/Languages
- Summary: Python's own image processing library
- Description: Python Imaging Library The Python Imaging Library (PIL) adds image processing capabilities to your Python interpreter. This library provides extensive file format support, an efficient internal representation, and powerful image processing capabilities. Details about licensing can be found from README 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

python-numeric-23.7-2.2.2 - python-numeric-23.7-2.2.2.el5_6.1

- Group: Development/Languages
- Summary: Numerical Extension to Python
- Description: Numeric is a python module that provides support for numerical operations.
- 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-0.400.3-11.el5 - python-virtinst-0.400.3-12.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

quota-3.13-4.el5 - quota-3.13-5.el5

- Group: System Environment/Base
- Summary: System administration tools for monitoring users' disk usage.
- Description: The quota package contains system administration tools for monitoring and limiting user and or group disk usage per filesystem.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rdesktop-1.6.0-3 - rdesktop-1.6.0-3.el5_6.2

- Group: User Interface/Desktops
- Summary: X client for remote desktop into Windows Terminal Server
- Description: rdesktop is an open source client for Windows NT Terminal Server and Windows 2000 & 2003 Terminal Services, capable of natively speaking Remote Desktop Protocol (RDP) in order to present the user's NT desktop. Unlike Citrix ICA, no server extensions are required.
- 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-5Client-5.6.0.3 - redhat-release-5Client-5.7.0.3

- 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-36 - redhat-release-notes-5Client-41

- 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

rhn-client-tools-0.4.20-46.el5 - rhn-client-tools-0.4.20-56.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.
- Added Dependencies:
  - desktop-file-utils
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rhnlib-2.5.22-5.el5 - rhnlib-2.5.22-6.el5

- Group: Development/Libraries
- Summary: Python libraries for the RHN project
- Description: rhnlib 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-4.7.0-5.el5 - rhnsd-4.7.0-10.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

rsync-2.6.8-3.1 - rsync-3.0.6-4.el5

- Group: Applications/Internet
- Summary: A program for synchronizing files over a network
- Description: Rsync uses a reliable algorithm to bring remote and host files into sync very quickly. Rsync is fast because it just sends the differences in the files over the network instead of sending the complete files. Rsync is often used as a very powerful mirroring process or just as a more capable replacement for the rcp command. A technical report which describes the rsync algorithm is included in this package.
- No added dependencies
- Removed Dependencies:
  - gcc
  - make
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rsyslog-3.22.1-3.el5_5.1 - rsyslog-3.22.1-3.el5_6.1

- Group: System Environment/Daemons

- Summary: Enhanced system logging and kernel message trapping daemon
- 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 sysklogd 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.
- No added dependencies
- Removed Dependencies:
  - autoconf
  - automake
  - libtool
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ruby-1.8.5-5.el5_4.8 - ruby-1.8.5-19.el5_6.1

- 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

sabayon-2.12.4-6.el5 - sabayon-2.12.4-7.el5

- Group: Applications/System
- Summary: Tool to maintain user profiles in a GNOME desktop
- Description: Sabayon is a tool to help sysadmins and user change and maintain the default behaviour of the GNOME desktop. This package contains the graphical tools which a sysadmin use to manage Sabayon profiles.
- 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-3.0.33-3.29.el5_5.1 - samba-3.0.33-3.29.el5_6.2

- 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

samba3x-3.5.4-0.70.el5 - samba3x-3.5.4-0.83.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.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

scim-1.4.4-41.el5 - scim-1.4.4-44.el5

- Group: System Environment/Libraries
- Summary: Smart Common Input Method platform
- Description: SCIM is a user friendly and full featured input method user interface and also a development platform to make life easier for Input Method 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

screen-4.0.3-3.el5 - screen-4.0.3-4.el5

- 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.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sed-4.1.5-5.fc6 - sed-4.1.5-8.el5

- Group: Applications/Text
- Summary: A GNU stream text editor.
- Description: The sed (Stream EDitor) editor is a stream or batch (non-interactive) editor. Sed takes text as input, performs an operation or set of operations on the text and outputs the modified text. The operations that sed performs (substitutions, deletions, insertions, etc.) can be specified in a script file or from the command 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

selinux-policy-2.4.6-300.el5 - selinux-policy-2.4.6-316.el5

- Group: System Environment/Base
- Summary: SELinux policy configuration
- Description: SELinux Reference Policy - modular.
- 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-4.0.17-18.el5 - shadow-utils-4.0.17-18.el5_6.1

- 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-1.7-9.49.el5 - sos-1.7-9.54.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

spamassassin-3.2.5-1.el5 - spamassassin-3.3.1-2.el5

- Group: Applications/Internet
- Summary: Spam filter for email which can be invoked from mail delivery agents.
- Description: SpamAssassin provides you with a way to reduce if not completely eliminate Unsolicited Commercial Email (SPAM) from your incoming email. It can be invoked by a MDA such as sendmail or postfix, or can be called from a procmail script, .forward file, etc. It uses a genetic-algorithm evolved scoring system to identify messages which look spammy, then adds headers to the message so they can be filtered by the user's mail reading software. This distribution includes the spamd/spamc components which create a server that considerably speeds processing of mail. To enable spamassassin, if you are receiving mail locally, simply add this line to your ~/.procmailrc: INCLUDERC=/etc/mail/spamassassin/spamassassin-default.rc To filter spam for all users, add that line to /etc/procmailrc (creating if necessary).
- Added Dependencies:
  - perl(Archive::Tar)
  - perl(NetAddr::IP)
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

spice-xpi-2.2-2.3.el5_5 - spice-xpi-2.2-2.3.el5_6.1

- Group: Applications/Internet
- Summary: SPICE extension for Mozilla
- Description: SPICE extension for mozilla allows the client to be used from a web browser.
- No added dependencies

- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sssd-1.2.1-39.el5 - sssd-1.5.1-37.el5

- Group: Applications/System
- Summary: System Security Services Daemon
- Description: Provides a set of daemons to manage access to remote directories and authentication mechanisms. It provides an NSS and PAM interface toward the system and a pluggable backend system to connect to multiple different account sources. It is also the basis to provide client auditing and policy services for projects like FreeIPA.
- Added Dependencies:
  - libcollection-devel
  - libdhash-devel >= 0.4.2
  - libini_config-devel >= 0.6.1
  - libnl-devel
  - nscd
  - openldap24-libs-devel
- Removed Dependencies:
  - openldap-devel
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

subversion-1.6.11-7.el5 - subversion-1.6.11-7.el5_6.4

- Group: Development/Tools

- Summary: Modern Version Control System designed to replace CVS
- Description: Subversion is a concurrent version control system which enables one or more users to collaborate in developing and maintaining a hierarchy of files and directories while keeping a history of all changes. Subversion only stores the differences between versions, instead of every complete file. Subversion is intended to be a compelling replacement for CVS.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sysfsutils-2.0.0-6 - sysfsutils-2.1.0-1.el5

- Group: Development/Tools
- Summary: sysfsutils, library interface to sysfs.
- Description: This package's purpose is to provide a set of utilities for interfacing with sysfs.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sysstat-7.0.2-3.el5_5.1 - sysstat-7.0.2-11.el5

- Group: Applications/System
- Summary: The sar and iostat system monitoring commands.
- Description: This package provides the sar and iostat commands for Linux. Sar and iostat enable system monitoring of disk, network, and other IO activity.
- 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-kickstart-2.6.19.8-2.el5 - system-config-kickstart-2.6.19.9-2.el5

- Group: System Environment/Base
- Summary: A graphical interface for making kickstart files.
- Description: Kickstart Configurator is a graphical tool for creating 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

system-config-lvm-1.1.5-8.el5 - system-config-lvm-1.1.5-9.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-netboot-0.1.45.1-1.el5 - system-config-netboot-0.1.45.1-3.el5

- Group: Applications/System
- Summary: network booting/install configuration utility (GUI)
- Description: system-config-netboot is a utility which allows you to configure diskless environments and network installations.
- 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-network-1.3.99.18-1.el5 - system-config-network-1.3.99.19-2.el5

- Group: Applications/System
- Summary: The GUI of the NEtwork Adminstration Tool
- Description: This is the GUI of the network configuration tool, supporting Ethernet, Wireless, TokenRing, ADSL, ISDN and PPP.
- 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-1.3-4.el5 - systemtap-1.3-8.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.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

talk-0.17-29.2.2 - talk-0.17-31.el5

- Group: Applications/Internet
- Summary: Talk client for one-on-one Internet chatting.
- Description: The talk package provides client programs for the Internet talk protocol, which allows you to chat with other users on different systems. Talk is a communication program which copies lines from one terminal to the terminal of another user. Install talk if you'd like to use talk for chatting with users on different 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

tetex-3.0-33.8.el5_5.6 - tetex-3.0-33.13.el5

- Group: Applications/Publishing
- Summary: The TeX text formatting system.
- Description: TeTeX is an implementation of TeX for Linux or UNIX systems. TeX takes a text file and a set of formatting commands as input and creates a typesetter-independent .dvi (DeVice Independent) file as output. Usually, TeX is used in conjunction with a higher level formatting package like LaTeX or PlainTeX, since TeX by itself is not very user-friendly. The

output format needn't to be DVI, but also PDF, when using pdflatex or similar tools. Install tetex if you want to use the TeX text formatting system. Consider to install tetex-latex (a higher level formatting package which provides an easier-to-use interface for TeX). Unless you are an expert at using TeX, you should also install the tetex-doc package, which includes the documentation for TeX.

- 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-2.0.0.24-13.el5_5 - thunderbird-2.0.0.24-18.el5_6

- 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

tomcat5-5.5.23-0jpp.16.el5 - tomcat5-5.5.23-0jpp.19.el5_6

- Group: Networking/Daemons
- Summary: Apache Servlet/JSP Engine, RI for Servlet 2.4/JSP 2.0 API
- Description: Tomcat is the servlet container that is used in the official Reference Implementation for the Java Servlet and JavaServer Pages technologies. The Java Servlet and JavaServer Pages specifications are developed by Sun under the Java Community Process. Tomcat is developed in an open and participatory environment and released under

the Apache Software License. Tomcat is intended to be a collaboration of the best-of-breed developers from around the world. We invite you to participate in this open development project. To learn more about getting involved, click here.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

totem-2.16.7-7.el5 - totem-2.16.7-7.el5_6.1

- Group: Applications/Multimedia
- Summary: Movie player for GNOME 2
- Description: Totem is simple movie player for the Gnome desktop. It features a simple playlist, a full-screen mode, seek and volume controls, as well as a pretty complete keyboard navigation.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

traceroute-2.0.1-5.el5 - traceroute-2.0.1-6.el5

- Group: Applications/Internet
- Summary: Traces the route taken by packets over an IPv4/IPv6 network
- Description: The traceroute utility displays the route used by IP packets on their way to a specified network (or Internet) host. Traceroute displays the IP number and host name (if possible) of the machines along the route taken by the packets. Traceroute is used as a network debugging tool. If you're having network connectivity problems, traceroute will show you where the trouble is coming from along the route. Install traceroute if you need a tool for diagnosing network connectivity problems.

- 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-2010l-1.el5 - tzdata-2011g-1.el5

- Group: System Environment/Base
- Summary: Timezone data
- Description: This package contains data files with rules for various time zones 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

udev-095-14.24.el5 - udev-095-14.27.el5

- Group: System Environment/Base
- Summary: A userspace implementation of devfs
- Description: The udev package contains an implementation of devfs in userspace using sysfs and netlink.
- 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-3.5.0-1.el5 - valgrind-3.5.0-5.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

virt-manager-0.6.1-13.el5 - virt-manager-0.6.1-14.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

- No added obsoletes
- No removed obsoletes

vnc-4.1.2-14.el5_5.4 - vnc-4.1.2-14.el5_6.6

- Group: User Interface/Desktops
- Summary: A remote display system.
- Description: Virtual Network Computing (VNC) is a remote display system 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. This package contains a client which will allow you to connect to other desktops running a VNC 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

vsftpd-2.0.5-16.el5_5.1 - vsftpd-2.0.5-21.el5

- 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

w3m-0.5.1-17.el5_5 - w3m-0.5.1-18.el5

- Group: Applications/Internet
- Summary: A pager with Web browsing abilities.
- Description: The w3m program is a pager (or text file viewer) that can also be used as a text-mode Web browser. W3m features include the following: when reading an HTML document, you can follow links and view images using an external image viewer; its internet message mode determines the type of document from the header; if the Content-Type field of the document is text/html, the document is displayed as an HTML document; you can change a URL description like 'http://hogege.net' in plain text into a link to that URL. If you want to display the inline images on w3m, you need to install w3m-img package as well.
- 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-0.14-7 - wdaemon-0.14-8

- 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

wireshark-1.0.15-1.el5_5.1 - wireshark-1.0.15-1.el5_6.4

- Group: Applications/Internet

- Summary: Network traffic analyzer
- Description: Wireshark is a network traffic analyzer for Unix-ish operating systems. This package lays base for libpcap, a packet capture and filtering library, contains command-line utilities, contains plugins and documentation for wireshark. A graphical user interface is packaged separately to GTK+ 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

xen-3.0.3-120.el5 - xen-3.0.3-132.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.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xinetd-2.3.14-10.el5 - xinetd-2.3.14-13.el5

- Group: System Environment/Daemons
- Summary: A secure replacement for inetd.

- Description: Xinetd is a secure replacement for inetd, the Internet services daemon. Xinetd provides access control for all services based on the address of the remote host and/or on time of access and can prevent denial-of-access attacks. Xinetd provides extensive logging, has no limit on the number of server arguments, and lets you bind specific services to specific IP addresses on your host machine. Each service has its own specific configuration file for Xinetd; the files are located in the /etc/xinetd.d directory.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xmlsec1-1.2.9-8.1.1 - xmlsec1-1.2.9-8.1.2

- 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-drv-ati-6.6.3-3.32.el5 - xorg-x11-drv-ati-6.6.3-3.33.el5

- Group: User Interface/X Hardware Support
- Summary: Xorg X11 ati video driver
- Description: X.Org X11 ati 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-mga-1.4.13-1.el5 - xorg-x11-drv-mga-1.4.13-2.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-qxl-0.0.12-1.2.el5 - xorg-x11-drv-qxl-0.0.12-2.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-1.3.0-8.2.el5 - xorg-x11-drv-vesa-1.3.0-8.3.el5

- Group: User Interface/X Hardware Support
- Summary: Xorg X11 vesa video driver
- Description: X.Org X11 vesa video driver.
- Added Dependencies:
  - xorg-x11-server-sdk >= 1.1.1-48.22
- Removed Dependencies:
  - xorg-x11-server-sdk >= 1.1.0-1
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xorg-x11-font-utils-7.1-2 - xorg-x11-font-utils-7.1-3

- Group: User Interface/X
- Summary: X.Org X11 font utilities
- Description: X.Org X11 font utilities required for font installation, conversion, and generation.
- 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-1.1.1-48.76.el5_5.2 - xorg-x11-server-1.1.1-48.76.el5_6.4

- Group: User Interface/X
- Summary: X.Org X11 X server
- Description: X.Org X11 X 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

xorg-x11-server-utils-7.1-4.fc6 - xorg-x11-server-utils-7.1-5.el5_6.2

- Group: User Interface/X
- Summary: X.Org X11 X server utilities
- Description: A collection of utilities used to tweak and query the runtime configuration of the X 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

xorg-x11-xfs-1.0.2-4 - xorg-x11-xfs-1.0.2-5.el5_6.1

- Group: System Environment/Daemons
- Summary: X.Org X11 xfs font server
- Description: X.Org X11 xfs font 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

xulrunner-1.9.2.13-3.el5 - xulrunner-1.9.2.18-2.el5_6

- Group: Applications/Internet
- Summary: XUL Runtime for Gecko Applications
- Description: XULRunner provides the XUL Runtime environment for Gecko 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

ypbind-1.19-12.el5 - ypbind-1.19-12.el5_6.1

- Group: System Environment/Daemons
- Summary: The NIS daemon which binds NIS clients to an NIS domain.
- Description: The Network Information Service (NIS) is a system that provides network information (login names, passwords, home directories, group information) to all of the machines on a network. NIS can allow users to log in 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 provides the ypbind daemon. The ypbind daemon binds NIS clients to an NIS domain. Ypbind must be running on any machines running NIS client programs. Install the ypbind package on any machines running NIS client programs (included in the yp-tools package). If you need an NIS server, you also need to install the ypserv package to a machine 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

ypserv-2.19-5.el5 - ypserv-2.19-5.el5_6.1

- Group: System Environment/Daemons
- Summary: The NIS (Network Information Service) server.
- Description: The Network Information Service (NIS) is a system that provides network information (login names, passwords, home directories, group information) to all of the machines on a network. NIS can allow users to log in 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 provides the NIS server, which will need to be running on your network. NIS clients do not need to be running the server. Install ypserv if you need an NIS server for your network. You also need to install the yp-tools and ypbind packages on any NIS client 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

yum-3.2.22-33.el5 - yum-3.2.22-37.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-0.5.4-17.el5 - yum-rhn-plugin-0.5.4-22.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

yum-utils-1.1.16-13.el5_4.1 - yum-utils-1.1.16-16.el5

- Group: Development/Tools
- Summary: Utilities based around the yum package manager
- Description: yum-utils is a collection of utilities and examples for the yum package manager. It includes utilities by different authors that make yum easier and more powerful to use. These tools include: debuginfo-install, package-cleanup, repoclosure, repodiff, repo-graph, repomanage, repoquery, repo-rss, reposync, repotrack, verifytree, yum-builddep, yum-complete-transaction, yumdownloader, yum-debug-dump and yum-groups-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

zlib-1.2.3-3 - zlib-1.2.3-4.el5

- Group: System Environment/Libraries
- Summary: The zlib compression and decompression library.
- Description: Zlib is a general-purpose, patent-free, lossless data compression library which is used by many different 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

A.2. SERVER

A.2.1. Added Packages

buildsys-macros-5-5.el5

- Group: Development/System
- Summary: Build system macros
- Description: Build system macros

cmake-2.6.4-5.el5.4

- Group: Development/Tools
- Summary: Cross-platform make system
- Description: CMake is used to control the software compilation process using simple platform and compiler independent configuration files. CMake generates native makefiles and workspaces that can be used in the compiler environment of your choice. CMake is quite sophisticated: it is possible to support complex environments requiring system configuration, preprocessor generation, code generation, and template instantiation.

ding-libs-0.1.2-10.el5

- Group: Development/Libraries
- Summary: "Ding is not GLib" assorted utility libraries
- Description: A set of helpful libraries used by projects such as SSSD.

jline-0.9.94-0.9.el5_6

- Group: Development/Libraries
- Summary: Java library for reading and editing user input in console applications
- Description: JLine is a java library for reading and editing user input in console applications. It features tab-completion, command history, password masking, customizable keybindings, and pass-through handlers to use to chain to other console applications.

libcxgb4-1.1.1-2.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.

man-pages-overrides-0.5.7.3-3.el5

- Group: Documentation
- Summary: Complementary and updated manual pages
- Description: A collection of manual ("man") pages to complement other packages or update those contained therein. Always have the latest version of this package installed.

openldap24-libs-2.4.23-5.el5

- Group: System Environment/Daemons
- Summary: LDAP support libraries
- 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.

openscap-0.7.2-1.el5

- Group: System Environment/Libraries
- Summary: Set of open source libraries enabling integration of the SCAP line of standards
- Description: OpenSCAP is a set of open source libraries providing an easier path for integration of the SCAP line of standards. SCAP is a line of standards managed by NIST with

the goal of providing a standard language for the expression of Computer Network Defense related information.

perl-NetAddr-IP-4.027-5.el5

- Group: Development/Libraries
- Summary: Manages IPv4 and IPv6 addresses and subnets
- Description: This module provides an object-oriented abstraction on top of IP addresses or IP subnets, that allows for easy manipulations. Version 4.xx of NetAdder::IP will will work older versions of Perl and does not use Math::BigInt as in previous versions.

python-ethtool-0.6-5.el5

- Group: System Environment/Libraries
- Summary: Ethernet settings python bindings
- Description: Python bindings for the ethtool kernel interface, that allows querying and changing of Ethernet card settings, such as speed, port, auto-negotiation, and PCI locations.

python-rhsm-0.95.5.5-1.el5

- Group: Development/Libraries
- Summary: A Python library to communicate with a Red Hat Unified Entitlement Platform
- Description: A small library for communicating with the REST interface of a Red Hat Unified Entitlement Platform. This interface is used for the management of system entitlements, certificates, and access to content.

python-simplejson-2.0.9-8.el5

- Group: System Environment/Libraries
- Summary: Simple, fast, extensible JSON encoder/decoder for Python
- Description: simplejson is a simple, fast, complete, correct and extensible JSON <http://json.org> encoder and decoder for Python 2.4+. It has no external dependencies. simplejson was formerly known as simple_json, but changed its name to comply with PEP 8 module naming guidelines. The encoder may be subclassed to provide serialization in any kind of situation, without any special support by the objects to be serialized (somewhat like pickle). The decoder can handle incoming JSON strings of any specified encoding (UTF-8 by default).

python-suds-0.4.1-2.el5

- Group: Development/Libraries
- Summary: A python SOAP client
- Description: The suds project is a python soap web services client lib. Suds leverages python meta programming to provide an intuitive API for consuming web services. Objectification of types defined in the WSDL is provided without class generation. Programmers rarely need to read the WSDL since services and WSDL based objects can be easily inspected.

rhino-1.7-0.7.r2.3.el5_6

- Group: Development/Libraries/Java
- Summary: JavaScript for Java
- Description: Rhino is an open-source implementation of JavaScript written entirely in Java. It is typically embedded into Java applications to provide scripting to end users.

subscription-manager-0.95.5.21-1.el5

- Group: System Environment/Base
- Summary: Tools and libraries for subscription and repository management
- Description: The Subscription Manager package provides programs and libraries to allow users to manage subscriptions and yum repositories from the Red Hat entitlement platform.

tcsh617-6.17-5.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.

virt-what-1.11-2.el5

- Group: Applications/Emulators
- Summary: Detect if we are running in a virtual machine
- Description: virt-what is a shell script which can be used to detect if the program is running in a virtual machine. The program prints out a list of "facts" about the virtual machine, derived from heuristics. One fact is printed per line. If nothing is printed and the script exits with code 0 (no error), then it can mean either that the program is running on bare-metal or the program is running inside a type of virtual machine which we don't know about or cannot detect. Current types of virtualization detected:
  - hyperv - Microsoft Hyper-V
  - kvm - Linux Kernel Virtual Machine (KVM)
  - openvz - OpenVZ or Virtuozzo
  - powervm_lx86 - IBM PowerVM Lx86 Linux/x86 emulator
  - qemu - QEMU (unaccelerated)
  - uml - User-Mode Linux (UML)
  - virtage - Hitachi Virtualization Manager (HVM) Virtage LPAR
  - virtualbox - VirtualBox

- virtualpc - Microsoft VirtualPC
- vmware - VMware
- xen - Xen
- xen-dom0 - Xen dom0 (privileged domain)
- xen-domU - Xen domU (paravirtualized guest domain)
- xen-hvm - Xen guest fully virtualized (HVM)

A.2.2. Dropped Packages

None

A.2.3. Updated Packages

NetworkManager-0.7.0-10.el5_5.2 - NetworkManager-0.7.0-13.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

SysVinit-2.86-15.el5 - SysVinit-2.86-17.el5

- Group: System Environment/Base
- Summary: Programs which control basic system processes.
- Description: The SysVinit package contains a group of processes that control the very basic functions of your system. SysVinit includes the init program, the first program started by the Linux kernel when the system boots. Init then controls the startup, running, and

shutdown of all other 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

anaconda-11.1.2.224-1 - anaconda-11.1.2.242-1

- 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.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

apr-1.2.7-11.el5_5.3 - apr-1.2.7-11.el5_6.5

- Group: System Environment/Libraries
- Summary: Apache Portable Runtime library
- Description: The mission of the Apache Portable Runtime (APR) is to provide a free library of C data structures and routines, forming a system portability layer to as many operating systems as possible, including Unices, MS Win32, BeOS and OS/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

authconfig-5.3.21-6.el5 - authconfig-5.3.21-7.el5

- Group: System Environment/Base
- Summary: Command line tool for setting up authentication from network services
- Description: Authconfig is a command line utility which can configure a workstation to use shadow (more secure) passwords. Authconfig can also configure a system to be a client for certain networked user information and authentication schemes.
- 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.rc2.143.el5_5.6 - autofs-5.0.1-0.rc2.156.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

avahi-0.6.16-9.el5_5 - avahi-0.6.16-10.el5_6

- 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

bash-3.2-24.el5 - bash-3.2-32.el5

- Group: System Environment/Shells
- Summary: The GNU Bourne Again shell (bash) version 3.2
- Description: The GNU Bourne Again shell (Bash) is a shell or command language interpreter that is compatible with the Bourne shell (sh). Bash incorporates useful features from the Korn shell (ksh) and the C shell (csh). Most sh scripts can be run by bash without modification. This package (bash) contains bash version 3.2, which improves POSIX compliance over previous versions.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

bind97-9.7.0-6.P2.el5 - bind97-9.7.0-6.P2.el5_6.3

- 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

booty-0.80.6-7 - booty-0.80.6-10

- 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

bridge-utils-1.1-2 - bridge-utils-1.1-3.el5

- Group: System Environment/Base

- Summary: Utilities for configuring the linux ethernet bridge
- Description: This package contains utilities for configuring the linux ethernet bridge. The linux ethernet bridge can be used for connecting multiple ethernet devices together. The connecting is fully transparent: hosts connected to one ethernet device see hosts connected to the other ethernet devices directly. Install bridge-utils if you want to use the linux ethernet bridge.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

busybox-1.2.0-7.el5 - busybox-1.2.0-10.el5

- Group: System Environment/Shells
- Summary: Statically linked binary providing simplified versions of system commands
- Description: Busybox is a single binary which includes versions of a large number of system commands, including a shell. This package can be very useful for recovering from certain types of system failures, particularly those involving broken shared libraries.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

certmonger-0.30-4.el5 - certmonger-0.42-1.el5

- Group: System Environment/Daemons
- Summary: Certificate status monitor and PKI enrollment client
- Description: Certmonger is a service which is primarily concerned with getting your system enrolled with a certificate authority (CA) and keeping it enrolled.

- Added Dependencies:
  - e2fsprogs-devel
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cman-2.0.115-68.el5 - cman-2.0.115-85.el5

- Group: System Environment/Base
- Summary: cman - The Cluster Manager
- Description: cman - The Cluster Manager
- Added Dependencies:
  - libxslt
  - pexpect
  - python-pycurl
  - python-suds
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

conga-0.12.2-24.el5 - conga-0.12.2-32.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

coreutils-5.97-23.el5_4.2 - coreutils-5.97-34.el5

- 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

cpuspeed-1.2.1-9.el5 - cpuspeed-1.2.1-10.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

cryptsetup-luks-1.0.3-5.el5 - cryptsetup-luks-1.0.3-8.el5

- Group: Applications/System
- Summary: A utility for setting up encrypted filesystems
- Description: This package contains cryptsetup, a utility for setting up encrypted filesystems using Device Mapper and the dm-crypt target.
- 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-1.3.7-26.el5 - cups-1.3.7-26.el5_6.1

- 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.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

curl-7.15.5-9.el5 - curl-7.15.5-9.el5_6.3

- 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_4.3 - cyrus-imapd-2.3.7-12.el5

- 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
- Removed Dependencies:
  - lm_sensors-devel
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dapl-2.0.25-2.el5_5.1 - dapl-2.0.25-2.el5_6.1

- 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.
- 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-1.1.2-14.el5 - dbus-1.1.2-15.el5_6

- 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

dejagnu-1.4.4-5.1 - dejagnu-1.4.4-7.el5

- Group: Development/Tools
- Summary: A front end for testing other programs.
- Description: DejaGnu is an Expect/Tcl based framework for testing other programs. DejaGnu has several purposes: to make it easy to write tests for any program; to allow you to write tests which will be portable to any host or target where a program must be tested; and to standardize the output format of all tests (making it easier to integrate the testing into software development).
- 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-1.02.55-2.el5 - device-mapper-1.02.63-4.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-0.4.7-42.el5 - device-mapper-multipath-0.4.7-46.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-3.0.5-23.el5_5.2 - dhcp-3.0.5-29.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

dmidecode-2.10-3.el5 - dmidecode-2.11-1.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.rc13-63.el5 - dmraid-1.0.0.rc13-65.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

dogtail-0.6.1-3.el5 - dogtail-0.6.1-4.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

e2fsprogs-1.39-23.el5_5.1 - e2fsprogs-1.39-33.el5

- Group: System Environment/Base
- Summary: Utilities for managing the second and third extended (ext2/ext3) filesystems
- Description: The e2fsprogs package contains a number of utilities for creating, checking, modifying, and correcting any inconsistencies in second and third extended (ext2/ext3) filesystems. E2fsprogs contains e2fsck (used to repair filesystem inconsistencies after an unclean shutdown), mke2fs (used to initialize a partition to contain an empty ext2 filesystem), debugfs (used to examine the internal structure of a filesystem, to manually repair a corrupted filesystem, or to create test cases for e2fsck), tune2fs (used to modify filesystem parameters), and most of the other core ext2fs filesystem utilities. You should install the e2fsprogs package if you need to manage the performance of an ext2 and/or ext3 filesystem.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

emacs-21.4-20.el5 - emacs-21.4-24.el5

- Group: Applications/Editors
- Summary: GNU Emacs text editor
- Description: Emacs is a powerful, customizable, self-documenting, modeless text editor. Emacs contains special code editing features, a scripting language (elisp), and the capability to read mail, news, and more without leaving the editor. This package provides an emacs binary with support for X windows.
- 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-5.4.4-13.el5 - etherboot-5.4.4-15.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
- 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-4.63-5.el5_5.2 - exim-4.63-10.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

finger-0.17-32.2.1.1 - finger-0.17-33

- Group: Applications/Internet
- Summary: The finger client.
- Description: Finger is a utility which allows users to see information about system users (login name, home directory, name, how long they've been logged in to the system, etc.). The finger package includes a standard finger client. You should install finger if you'd like to retrieve finger information from other 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

firefox-3.6.13-2.el5 - firefox-3.6.18-1.el5_6

- 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 >= 1.9.2.18-1
- Removed Dependencies:
  - xulrunner-devel >= 1.9.2.13-3
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

fonts-indic-2.3.1-1.el5 - fonts-indic-2.3.1.1-2.el5

- Group: User Interface/X
- Summary: Free Indian truetype/opentype fonts
- Description: This package provides the Hindi, Bengali, Gujarati, Punjabi, Tamil, Kannada,\ Malayalam, Oriya, Telugu TrueType/Opentype fonts.
- 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-4.1.2-50.el5 - gcc-4.1.2-51.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

gdb-7.0.1-32.el5 - gdb-7.0.1-37.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.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gfs-utils-0.1.20-8.el5 - gfs-utils-0.1.20-10.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-0.1.62-28.el5 - gfs2-utils-0.1.62-31.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

giflib-4.1.3-7.1.el5_3.1 - giflib-4.1.3-7.3.3.el5

- Group: System Environment/Libraries
- Summary: Library for manipulating GIF format image files
- Description: The giflib package contains a shared library of functions for loading and saving GIF format image files. It is API and ABI compatible with libungif, the library which supported uncompressed GIFs while the Unisys LZW patent was in effect. Install the giflib package if you need to write programs that use GIF files. You should also install the giflib-utils package if you need some simple utilities to manipulate GIFs.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

gimp-2.2.13-2.0.7.el5 - gimp-2.2.13-2.0.7.el5_6.2

- Group: Applications/Multimedia
- Summary: GNU Image Manipulation Program
- Description: GIMP (GNU Image Manipulation Program) is a powerful image composition and editing program, which can be extremely useful for creating logos and other graphics for webpages. GIMP has many of the tools and filters you would expect to find in similar commercial offerings, and some interesting extras as well. GIMP provides a large image manipulation toolbox, including channel operations and layers, effects, sub-pixel imaging and anti-aliasing, and conversions, all with multi-level undo.
- 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-2.5-58 - glibc-2.5-65

- 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-screensaver-2.16.1-8.el5_5.2 - gnome-screensaver-2.16.1-8.el5_6.3

- Group: Amusements/Graphics
- Summary: GNOME Screensaver
- Description: gnome-screensaver is a screen saver and locker that aims to have simple, sane, secure defaults and be well integrated with the desktop.
- 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-terminal-2.16.0-5.3.el5 - gnome-terminal-2.16.0-5.3.el5_6.1

- Group: User Interface/Desktops
- Summary: GNOME Terminal
- Description: GNOME terminal emulator application.
- 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-vfs2-2.16.2-6.el5_5.1 - gnome-vfs2-2.16.2-8.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.

- 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-1.3.5-11.el5_4.1 - gzip-1.3.5-13.el5

- 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

hplip-1.6.7-6.el5 - hplip-1.6.7-6.el5_6.1

- Group: System Environment/Daemons
- Summary: HP Linux Imaging and Printing Project
- Description: The Hewlett-Packard Linux Imaging and Printing Project provides drivers for HP printers and multi-function peripherals.
- No added dependencies

- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

hplip3-3.9.8-11.el5 - hplip3-3.9.8-11.el5_6.1

- Group: System Environment/Daemons
- Summary: HP Linux Imaging and Printing Project
- Description: The Hewlett-Packard Linux Imaging and Printing Project provides drivers for HP printers and multi-function peripherals.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

httpd-2.2.3-45.el5 - httpd-2.2.3-53.el5

- Group: System Environment/Daemons
- Summary: Apache HTTP Server
- Description: The Apache HTTP Server is a powerful, efficient, and extensible web 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

hwdata-0.213.22-1.el5 - hwdata-0.213.24-1.el5

- 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

initscripts-8.45.33-1.el5 - initscripts-8.45.38-2.el5

- Group: System Environment/Base
- Summary: The inittab file and the /etc/init.d scripts.
- Description: The initscripts package contains the basic system scripts used to boot your Red Hat system, change runlevels, and shut the system down cleanly. Initscripts also contains the scripts that activate and deactivate most network interfaces.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ipa-client-2.0-10.el5 - ipa-client-2.0-14.el5

- Group: System Environment/Base

- Summary: IPA authentication for use on clients
- Description: IPA is an integrated solution to provide centrally managed Identity (machine, user, virtual machines, groups, authentication credentials), Policy (configuration settings, access control information) and Audit (events, logs, analysis thereof).
- Added Dependencies:
  - authconfig
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

iprutils-2.3.0-2.el5 - iprutils-2.3.4-1.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

ipvsadm-1.24-12.el5 - ipvsadm-1.24-13.el5

- Group: Applications/System
- Summary: Utility to administer the Linux Virtual Server
- Description: ipvsadm is a utility to administer the IP Virtual Server services offered by the Linux 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

iscsi-initiator-utils-6.2.0.872-6.el5 - iscsi-initiator-utils-6.2.0.872-10.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
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

java-1.6.0-openjdk-1.6.0.0-1.16.b17.el5 - java-1.6.0-openjdk-1.6.0.0-1.22.1.9.8.el5_6

- Group: Development/Languages
- Summary: OpenJDK Runtime Environment
- Description: The OpenJDK runtime environment.
- Added Dependencies:
  - ant-nodeps
  - redhat-lsb
  - rhino

- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

jwhois-3.2.3-11.el5 - jwhois-3.2.3-12.el5

- Group: Applications/Internet
- Summary: Internet whois/nicname client.
- Description: A whois client that accepts both traditional and finger-style queries.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

kdebase-3.5.4-22.el5 - kdebase-3.5.4-24.el5

- Group: User Interface/Desktops
- Summary: K Desktop Environment - core files
- Description: Core applications for the K Desktop Environment. Included are: kdm (replacement for xdm), kwin (window manager), konqueror (filemanager, web browser, ftp client, ...), konsole (xterm replacement), kpanel (application starter and desktop pager), kaudio (audio server), kdehelp (viewer for kde help files, info and man pages), kthememgr (system for managing alternate theme packages) plus other KDE components (kcheckpass, kikbd, kscreensaver, kcontrol, kfind, kfontmanager, kmenuedit).
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

kdenetwork-3.5.4-9.el5 - kdenetwork-3.5.4-13.el5_6.1

- Group: Applications/Internet
- Summary: K Desktop Environment - Network Applications
- Description: Networking applications for the K Desktop 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

kernel-2.6.18-238.el5 - kernel-2.6.18-274.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-126.el5 - kexec-tools-1.102pre-126.el5_6.6

- Group: Applications/System
- Summary: The kexec/kdump userspace component.
- 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

krb5-1.6.1-55.el5 - krb5-1.6.1-62.el5

- 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-20100202-1.el5_5.1 - ksh-20100202-1.el5_6.6

- 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

kvm-83-224.el5 - kvm-83-239.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-debug-devel = 2.6.18-269.el5
  - kernel-devel = 2.6.18-269.el5
- Removed Dependencies:
  - kernel-debug-devel = 2.6.18-237.el5
  - kernel-devel = 2.6.18-237.el5
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

lapack-3.0-37.el5 - lapack-3.0-38.el5

- Group: Development/Libraries

- Summary: The LAPACK libraries for numerical linear algebra
- Description: LAPACK (Linear Algebra PACKage) is a standard library for numerical linear algebra. LAPACK provides routines for solving systems of simultaneous linear equations, least-squares solutions of linear systems of equations, eigenvalue problems, and singular value problems. Associated matrix factorizations (LU, Cholesky, QR, SVD, Schur, and generalized Schur) and related computations (i.e., reordering of Schur factorizations and estimating condition numbers) are also included. LAPACK can handle dense and banded matrices, but not general sparse matrices. Similar functionality is provided for real and complex matrices in both single and double precision. LAPACK is coded in Fortran77 and built with gcc.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libdhcp-1.20-10.el5 - libdhcp-1.20-11.el5

- Group: Development/Libraries
- Summary: A library for network interface configuration with DHCP
- Description: libdhcp enables programs to invoke and control the Dynamic Host Configuration Protocol (DHCP) clients: the Internet Software Consortium (ISC) IPv4 DHCP client library, libdhcp4client, and the IPv6 DHCPv6 client library, libdhcp6client, and provides Network Interface Configuration (NIC) services for network parameter autoconfiguration with DHCP.
- Added Dependencies:
  - dhcp-devel >= 12:3.0.5-26
  - libdhcp4client-devel >= 12:3.0.5-26
- Removed Dependencies:
  - dhcp-devel >= 12:3.0.5-13
  - libdhcp4client-devel >= 12:3.0.5-13
- No added provides
- No removed provides
- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

libmlx4-1.0.1-5.el5 - libmlx4-1.0.1-6.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.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libtdb-1.2.1-5.el5 - libtdb-1.2.1-6.el5

- Group: System Environment/Daemons
- Summary: The tdb library
- Description: A library that implements a trivial database.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libtiff-3.8.2-7.el5_5.5 - libtiff-3.8.2-7.el5_6.7

- Group: System Environment/Libraries

- Summary: Library of functions for manipulating TIFF format image files
- Description: The libtiff package contains a library of functions for manipulating TIFF (Tagged Image File Format) image format files. TIFF is a widely used file format for bitmapped images. TIFF files usually end in the .tif extension and they are often quite large. The libtiff package should be installed if you need to manipulate TIFF format image 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

libuser-0.54.7-2.1.el5_4.1 - libuser-0.54.7-2.1.el5_5.2

- 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:
  - openldap-clients
  - openldap-servers
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libvirt-0.8.2-15.el5 - libvirt-0.8.2-22.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

libxml2-2.6.26-2.1.2.8.el5_5.1 - libxml2-2.6.26-2.1.12

- Group: Development/Libraries
- Summary: Library providing XML and HTML support
- Description: This library allows to manipulate XML files. It includes support to read, modify and write XML and HTML files. There is DTDs support this includes parsing and validation even with complex DtDs, either at parse time or later once the document has been modified. The output can be a simple SAX stream or and in-memory DOM like representations. In this case one can use the built-in XPath and XPointer implementation to select subnodes or ranges. A flexible Input/Output mechanism is available, with existing HTTP and FTP modules and combined to an URI 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

linuxwacom-0.7.8.3-10.el5 - linuxwacom-0.7.8.3-11.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

logrotate-3.7.4-9.el5_5.2 - logrotate-3.7.4-12

- Group: System Environment/Base
- Summary: Rotates, compresses, removes and mails system log files.
- Description: The logrotate utility is designed to simplify the administration of log files on a system which generates a lot of log files. Logrotate allows for the automatic rotation compression, removal and mailing of log files. Logrotate can be set to handle a log file daily, weekly, monthly or when the log file gets to a certain size. Normally, logrotate runs as a daily cron job. Install the logrotate package if you need a utility to deal with the log files on your 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

logwatch-7.3-8.el5 - logwatch-7.3-9.el5_6

- 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

lvm2-2.02.74-5.el5 - lvm2-2.02.84-6.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.
- Added Dependencies:
  - device-mapper >= 1.02.63-2
- Removed Dependencies:
  - device-mapper >= 1.02.55-2
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

lvm2-cluster-2.02.74-3.el5 - lvm2-cluster-2.02.84-6.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 >= 1.02.63-2
- Removed Dependencies:
    - device-mapper >= 1.02.55-2
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

m2crypto-0.16-6.el5.8 - m2crypto-0.16-8.el5

- Group: System Environment/Libraries
- Summary: Support for using OpenSSL in python scripts
- Description: This package allows you to call OpenSSL functions from python scripts.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mailman-2.1.9-6.el5 - mailman-2.1.9-6.el5_6.1

- Group: Applications/Internet
- Summary: Mailing list manager with built in Web access.
- Description: Mailman is software to help manage email discussion lists, much like Majordomo and Smartmail. Unlike most similar products, Mailman gives each mailing list a webpage, and allows users to subscribe, unsubscribe, etc. over the Web. Even the list manager can administer his or her list entirely from the Web. Mailman also integrates most things people want to do with mailing lists, including archiving, mail <-> news gateways, and so on. Documentation can be found in: /usr/share/doc/mailman-2.1.9 When the package has finished installing, you will need to perform some additional installation steps, these are described in: /usr/share/doc/mailman-2.1.9/INSTALL.REDHAT
- 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-1.6d-1.1 - man-1.6d-2.el5

- Group: System Environment/Base
- Summary: A set of documentation tools: man, apropos and whatis.
- Description: The man package includes three tools for finding information and/or documentation about your Linux system: man, apropos, and whatis. The man system formats and displays on-line manual pages about commands or functions on your system. Apropos searches the whatis database (containing short descriptions of system commands) for a string. Whatis searches its own database for a complete word. The man package should be installed on your system because it is the primary way to find documentation on a Linux 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

mcelog-0.9pre-1.29.el5 - mcelog-0.9pre-1.32.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
- No added obsoletes
- No removed obsoletes

mkinitrd-5.1.19.6-68.el5 - mkinitrd-5.1.19.6-71.el5

- 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

mod_authz_ldap-0.26-9.el5_5.1 - mod_authz_ldap-0.26-11.el5

- Group: System Environment/Daemons
- Summary: LDAP authorization module for the Apache HTTP Server
- Description: The mod_authz_ldap package provides support for authenticating users of the Apache HTTP server against an LDAP database. mod_authz_ldap features the ability to authenticate users based on the SSL client certificate presented, and also supports password aging, and authentication based on role or by configured filters.
- No added dependencies
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mod_nss-1.0.8-3.el5 - mod_nss-1.0.8-4.el5_6.1

- Group: System Environment/Daemons
- Summary: SSL/TLS module for the Apache HTTP server
- Description: The mod_nss module provides strong cryptography for the Apache Web server via the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols using the Network Security Services (NSS) security 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

mysql-5.0.77-4.el5_5.4 - mysql-5.0.77-4.el5_6.6

- 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-2.16.2-7.el5 - nautilus-2.16.2-10.el5

- Group: User Interface/Desktops
- Summary: Nautilus is a file manager for GNOME.
- Description: Nautilus integrates access to files, applications, media, Internet-based resources and the Web. Nautilus delivers a dynamic and rich user experience. Nautilus is an free software project developed under the GNU General Public License and is a core component of the GNOME desktop 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

net-snmp-5.3.2.2-9.el5_5.1 - net-snmp-5.3.2.2-14.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

nfs-utils-1.0.9-50.el5 - nfs-utils-1.0.9-54.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
- No removed obsoletes

nss-3.12.8-1.el5 - nss-3.12.8-4.el5_6

- Group: System Environment/Libraries
- Summary: Network Security Services
- Description: Network Security Services (NSS) is a set of libraries designed to support cross-platform development of security-enabled client and server applications. Applications built with NSS can support SSL v2 and v3, TLS, PKCS #5, PKCS #7, PKCS #11, PKCS #12, S/MIME, X.509 v3 certificates, and other security standards.
- 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-253-37.el5 - nss_ldap-253-42.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:
  - openssl-devel >= 0.9.8e-18
- Removed Dependencies:
  - openssl-devel
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ntp-4.2.2p1-9.el5_4.1 - ntp-4.2.2p1-15.el5

- 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-0.9.8-11.el5 - numactl-0.9.8-12.el5_6

- 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

openais-0.80.6-28.el5 - openais-0.80.6-30.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-1.4.1-5.el5 - openib-1.4.1-6.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-2.3.43-12.el5_5.3 - openldap-2.3.43-12.el5_6.7

- 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

opensm-3.3.3-1.el5 - opensm-3.3.3-2.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.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openssh-4.3p2-72.el5 - openssh-4.3p2-72.el5_6.3

- 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_5.7 - openssl-0.9.8e-20.el5

- 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_5.3 - openswan-2.6.21-5.el5_6.4

- 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

pam_krb5-2.2.14-18.el5 - pam_krb5-2.2.14-21.el5

- Group: System Environment/Base

- 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

pango-1.14.9-8.el5 - pango-1.14.9-8.el5_6.2

- Group: System Environment/Libraries
- Summary: System for layout and rendering of internationalized text
- Description: Pango is a system for layout and rendering of internationalized text.
- 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-0.6.6-19.el5 - paps-0.6.6-20.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-1.8.1-27.el5 - parted-1.8.1-28.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

pcre-6.6-6.el5 - pcre-6.6-6.el5_6.1

- Group: System Environment/Libraries
- Summary: Perl-compatible regular expression library
- Description: Perl-compatible regular expression library. PCRE has its own native API, but a set of "wrapper" functions that are based on the POSIX API are also supplied in the library libpcreposix. Note that this just provides a POSIX calling interface to PCRE: the regular expressions themselves still follow Perl syntax and semantics. The header file for the POSIX-style functions is called pcreposix.h.
- 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-5.8.8-32.el5_5.2 - perl-5.8.8-32.el5_6.3

- Group: Development/Languages
- Summary: The Perl programming language
- Description: Perl is a high-level programming language with roots in C, sed, awk and shell scripting. Perl is good at handling processes and files, and is especially good at handling text. Perl's hallmarks are practicality and efficiency. While it is used to do a lot of different things, Perl's most common applications are system administration utilities and web programming. A large proportion of the CGI scripts on the web are written in Perl. You need the perl package installed on your system so that your system can handle Perl scripts. Install this package if you want to program in Perl or enable your system to handle Perl scripts.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

php53-5.3.3-1.el5 - php53-5.3.3-1.el5_6.1

- Group: Development/Languages
- Summary: PHP scripting language for creating dynamic web sites
- 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

piranha-0.8.4-19.el5 - piranha-0.8.4-22.el5

- Group: System Environment/Base
- Summary: Cluster administation 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

poppler-0.5.4-4.4.el5_5.14 - poppler-0.5.4-4.4.el5_6.17

- 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

postfix-2.3.3-2.1.el5_2 - postfix-2.3.3-2.3.el5_6

- Group: System Environment/Daemons
- Summary: Postfix Mail Transport Agent
- Description: Postfix is a Mail Transport Agent (MTA), supporting LDAP, SMTP AUTH (SASL), TLS
- 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-8.1.22-1.el5_5.1 - postgresql-8.1.23-1.el5_6.1

- 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

postgresql84-8.4.5-1.el5_5.1 - postgresql84-8.4.7-1.el5_6.1

- 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.
- 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-3.2.7-16.el5 - procps-3.2.7-17.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 pdwx. 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

psmisc-22.2-7 - psmisc-22.2-7.el5_6.2

- Group: Applications/System
- Summary: Utilities for managing processes on your system.
- Description: The psmisc package contains utilities for managing processes on your system: pstree, killall and fuser. The pstree command displays a tree structure of all of the running processes on your system. The killall command sends a specified signal (SIGTERM if nothing is specified) to processes identified by name. The fuser command identifies the PIDs of processes that are using specified files or 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

pyOpenSSL-0.6-1.p24.7.2.2 - pyOpenSSL-0.6-2.el5

- Group: Development/Libraries
- Summary: Python wrapper module around the OpenSSL library

- Description: High-level wrapper around a subset of the OpenSSL library, includes * SSL.Connection objects, wrapping the methods of Python's portable sockets * Callbacks written in Python * Extensive error-handling mechanism, mirroring OpenSSL's error codes ... and much more ;)
- 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-0.43.8-1.el5 - pykickstart-0.43.9-1.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-2.4.3-43.el5 - python-2.4.3-44.el5

- Group: Development/Languages
- Summary: An interpreted, interactive, object-oriented programming language.
- Description: Python is an interpreted, interactive, object-oriented programming language often compared to Tcl, Perl, Scheme or Java. Python includes modules, classes, exceptions, very high level dynamic data types and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems (X11, Motif, Tk, Mac and MFC). Programmers can write new built-in modules for Python in C or C++. Python can be used as an extension language for applications that need a programmable interface. This

package contains most of the standard Python modules, as well as modules for interfacing to the Tix widget set for Tk and RPM. Note that documentation for Python is provided in the python-docs 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

python-imaging-1.1.5-5.el5 - python-imaging-1.1.5-7.el5

- Group: Development/Languages
- Summary: Python's own image processing library
- Description: Python Imaging Library The Python Imaging Library (PIL) adds image processing capabilities to your Python interpreter. This library provides extensive file format support, an efficient internal representation, and powerful image processing capabilities. Details about licensing can be found from README 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

python-numeric-23.7-2.2.2 - python-numeric-23.7-2.2.2.el5_6.1

- Group: Development/Languages
- Summary: Numerical Extension to Python
- Description: Numeric is a python module that provides support for numerical operations.
- 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-0.400.3-11.el5 - python-virtinst-0.400.3-12.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

quota-3.13-4.el5 - quota-3.13-5.el5

- Group: System Environment/Base
- Summary: System administration tools for monitoring users' disk usage.
- Description: The quota package contains system administration tools for monitoring and limiting user and or group disk usage per filesystem.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

rdesktop-1.6.0-3 - rdesktop-1.6.0-3.el5_6.2

- Group: User Interface/Desktops
- Summary: X client for remote desktop into Windows Terminal Server
- Description: rdesktop is an open source client for Windows NT Terminal Server and Windows 2000 & 2003 Terminal Services, capable of natively speaking Remote Desktop Protocol (RDP) in order to present the user's NT desktop. Unlike Citrix ICA, no server extensions are required.
- 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-5.6.0.3 - redhat-release-5Server-5.7.0.3

- 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-36 - redhat-release-notes-5Server-41

- 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-2.0.52-9.el5 - rgmanager-2.0.52-21.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
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rhn-client-tools-0.4.20-46.el5 - rhn-client-tools-0.4.20-56.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.

- Added Dependencies:
  - desktop-file-utils
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rhnlib-2.5.22-5.el5 - rhnlib-2.5.22-6.el5

- Group: Development/Libraries
- Summary: Python libraries for the RHN project
- Description: rhnlib 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-4.7.0-5.el5 - rhnsd-4.7.0-10.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

rsync-2.6.8-3.1 - rsync-3.0.6-4.el5

- Group: Applications/Internet
- Summary: A program for synchronizing files over a network
- Description: Rsync uses a reliable algorithm to bring remote and host files into sync very quickly. Rsync is fast because it just sends the differences in the files over the network instead of sending the complete files. Rsync is often used as a very powerful mirroring process or just as a more capable replacement for the rcp command. A technical report which describes the rsync algorithm is included in this package.
- No added dependencies
- Removed Dependencies:
  - gcc
  - make
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rsyslog-3.22.1-3.el5_5.1 - rsyslog-3.22.1-3.el5_6.1

- Group: System Environment/Daemons
- Summary: Enhanced system logging and kernel message trapping daemon
- 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 sysklogd 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.
- No added dependencies
- Removed Dependencies:

    - autoconf
    - automake
    - libtool
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ruby-1.8.5-5.el5_4.8 - ruby-1.8.5-19.el5_6.1

- 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

s390utils-1.8.1-11.el5 - s390utils-1.8.1-16.el5

- Group: System Environment/Base
- Summary: Linux/390 specific utilities
- Description: This package contains utilities related to Linux for S/390. The most important programs contained in this package are: - The cmstools suite to list, check, copy and cat files from a CMS volume. - chccwdev, a script to generically change attributes of a ccw device. - dasdfmt, which is used to low-level format eckd-dasds with either the classic linux disk layout or the new z/OS compatible disk layout. - dasdview, which displays DASD and VTOC information and dumps the content of a DASD to the console. - fdasd, which is used to create or modify partitions on eckd-dasds formatted with the z/OS compatible disk layout. - osasnmpd, a subagent for net-snmp to access the OSA hardware. - qetharp to query and

purge address data in the OSA and HiperSockets hardware - qethconf to configure IBM QETH function IPA, VIPA and Proxy ARP. - src_vipa.sh to start applications using VIPA capabilities - tunedasd, a tool to adjust tunable parameters on DASD devices - vmconvert, a tool to convert vm dumps to lkcd compatible dumps. - vmcp, a tool to send CP commands from a Linux guest to the VM. - vmur, a tool to work with z/VM spool file queues (reader, punch, printer). - zipl, which is used to make either dasds or tapes bootable for system IPL or system dump. - zdump, which is used to retrieve system dumps from either tapes or dasds. - ziomon tools to collect data for zfcp performance analysis and report. - iucvterm, a z/VM IUCV terminal applications. - cpuplugd, a daemon that manages CPU and memory resources based on a set of rules. - dumpconf, the dump device used for system dump in case a kernel panic occurs. - mon_statd, pair of Linux - z/VM monitoring daemons. - ipl_tools, tool set to configure and list reipl and shutdown actions. - cpi, a service to set the system and sysplex names from the Linux guest to the HMC/SE using the Control Program Identification 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

sabayon-2.12.4-6.el5 - sabayon-2.12.4-7.el5

- Group: Applications/System
- Summary: Tool to maintain user profiles in a GNOME desktop
- Description: Sabayon is a tool to help sysadmins and user change and maintain the default behaviour of the GNOME desktop. This package contains the graphical tools which a sysadmin use to manage Sabayon profiles.
- 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-3.0.33-3.29.el5_5.1 - samba-3.0.33-3.29.el5_6.2

- 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

samba3x-3.5.4-0.70.el5 - samba3x-3.5.4-0.83.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.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

scim-1.4.4-41.el5 - scim-1.4.4-44.el5

- Group: System Environment/Libraries
- Summary: Smart Common Input Method platform
- Description: SCIM is a user friendly and full featured input method user interface and also a development platform to make life easier for Input Method 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

screen-4.0.3-3.el5 - screen-4.0.3-4.el5

- 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.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

scsi-target-utils-1.0.8-0.el5 - scsi-target-utils-1.0.14-1.el5

- 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
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sed-4.1.5-5.fc6 - sed-4.1.5-8.el5

- Group: Applications/Text
- Summary: A GNU stream text editor.
- Description: The sed (Stream EDitor) editor is a stream or batch (non-interactive) editor. Sed takes text as input, performs an operation or set of operations on the text and outputs the modified text. The operations that sed performs (substitutions, deletions, insertions, etc.) can be specified in a script file or from the command 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

selinux-policy-2.4.6-300.el5 - selinux-policy-2.4.6-316.el5

- Group: System Environment/Base
- Summary: SELinux policy configuration
- Description: SELinux Reference Policy - modular.
- 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-4.0.17-18.el5 - shadow-utils-4.0.17-18.el5_6.1

- 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-1.7-9.49.el5 - sos-1.7-9.54.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

spamassassin-3.2.5-1.el5 - spamassassin-3.3.1-2.el5

- Group: Applications/Internet
- Summary: Spam filter for email which can be invoked from mail delivery agents.
- Description: SpamAssassin provides you with a way to reduce if not completely eliminate Unsolicited Commercial Email (SPAM) from your incoming email. It can be invoked by a MDA such as sendmail or postfix, or can be called from a procmail script, .forward file, etc. It uses a genetic-algorithm evolved scoring system to identify messages which look spammy, then adds headers to the message so they can be filtered by the user's mail reading software. This distribution includes the spamd/spamc components which create a server that considerably speeds processing of mail. To enable spamassassin, if you are receiving mail locally, simply add this line to your ~/.procmailrc: INCLUDERC=/etc/mail/spamassassin/spamassassin-default.rc To filter spam for all users, add that line to /etc/procmailrc (creating if necessary).
- Added Dependencies:
  - perl(Archive::Tar)
  - perl(NetAddr::IP)
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sssd-1.2.1-39.el5 - sssd-1.5.1-37.el5

- Group: Applications/System
- Summary: System Security Services Daemon
- Description: Provides a set of daemons to manage access to remote directories and authentication mechanisms. It provides an NSS and PAM interface toward the system and a

pluggable backend system to connect to multiple different account sources. It is also the basis to provide client auditing and policy services for projects like FreeIPA.

- Added Dependencies:
  - libcollection-devel
  - libdhash-devel >= 0.4.2
  - libini_config-devel >= 0.6.1
  - libnl-devel
  - nscd
  - openldap24-libs-devel
- Removed Dependencies:
  - openldap-devel
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

subversion-1.6.11-7.el5 - subversion-1.6.11-7.el5_6.4

- Group: Development/Tools
- Summary: Modern Version Control System designed to replace CVS
- Description: Subversion is a concurrent version control system which enables one or more users to collaborate in developing and maintaining a hierarchy of files and directories while keeping a history of all changes. Subversion only stores the differences between versions, instead of every complete file. Subversion is intended to be a compelling replacement for CVS.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

sysfsutils-2.0.0-6 - sysfsutils-2.1.0-1.el5

- Group: Development/Tools
- Summary: sysfsutils, library interface to sysfs.
- Description: This package's purpose is to provide a set of utilities for interfacing with sysfs.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sysstat-7.0.2-3.el5_5.1 - sysstat-7.0.2-11.el5

- Group: Applications/System
- Summary: The sar and iostat system monitoring commands.
- Description: This package provides the sar and iostat commands for Linux. Sar and iostat enable system monitoring of disk, network, and other IO activity.
- 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-1.0.57-7 - system-config-cluster-1.0.57-9

- 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 configuuration 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-kickstart-2.6.19.8-2.el5 - system-config-kickstart-2.6.19.9-2.el5

- Group: System Environment/Base
- Summary: A graphical interface for making kickstart files.
- Description: Kickstart Configurator is a graphical tool for creating 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

system-config-lvm-1.1.5-8.el5 - system-config-lvm-1.1.5-9.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-netboot-0.1.45.1-1.el5 - system-config-netboot-0.1.45.1-3.el5

- Group: Applications/System
- Summary: network booting/install configuration utility (GUI)
- Description: system-config-netboot is a utility which allows you to configure diskless environments and network installations.
- 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-network-1.3.99.18-1.el5 - system-config-network-1.3.99.19-2.el5

- Group: Applications/System
- Summary: The GUI of the NEtwork Adminstration Tool
- Description: This is the GUI of the network configuration tool, supporting Ethernet, Wireless, TokenRing, ADSL, ISDN and PPP.
- 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-1.3-4.el5 - systemtap-1.3-8.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.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

talk-0.17-29.2.2 - talk-0.17-31.el5

- Group: Applications/Internet
- Summary: Talk client for one-on-one Internet chatting.
- Description: The talk package provides client programs for the Internet talk protocol, which allows you to chat with other users on different systems. Talk is a communication program which copies lines from one terminal to the terminal of another user. Install talk if you'd like to use talk for chatting with users on different 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

tetex-3.0-33.8.el5_5.6 - tetex-3.0-33.13.el5

- Group: Applications/Publishing
- Summary: The TeX text formatting system.

- Description: TeTeX is an implementation of TeX for Linux or UNIX systems. TeX takes a text file and a set of formatting commands as input and creates a typesetter-independent .dvi (DeVice Independent) file as output. Usually, TeX is used in conjunction with a higher level formatting package like LaTeX or PlainTeX, since TeX by itself is not very user-friendly. The output format needn't to be DVI, but also PDF, when using pdflatex or similar tools. Install tetex if you want to use the TeX text formatting system. Consider to install tetex-latex (a higher level formatting package which provides an easier-to-use interface for TeX). Unless you are an expert at using TeX, you should also install the tetex-doc package, which includes the documentation for TeX.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

tomcat5-5.5.23-0jpp.16.el5 - tomcat5-5.5.23-0jpp.19.el5_6

- Group: Networking/Daemons
- Summary: Apache Servlet/JSP Engine, RI for Servlet 2.4/JSP 2.0 API
- Description: Tomcat is the servlet container that is used in the official Reference Implementation for the Java Servlet and JavaServer Pages technologies. The Java Servlet and JavaServer Pages specifications are developed by Sun under the Java Community Process. Tomcat is developed in an open and participatory environment and released under the Apache Software License. Tomcat is intended to be a collaboration of the best-of-breed developers from around the world. We invite you to participate in this open development project. To learn more about getting involved, click here.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

totem-2.16.7-7.el5 - totem-2.16.7-7.el5_6.1

- Group: Applications/Multimedia
- Summary: Movie player for GNOME 2
- Description: Totem is simple movie player for the Gnome desktop. It features a simple playlist, a full-screen mode, seek and volume controls, as well as a pretty complete keyboard navigation.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

traceroute-2.0.1-5.el5 - traceroute-2.0.1-6.el5

- Group: Applications/Internet
- Summary: Traces the route taken by packets over an IPv4/IPv6 network
- Description: The traceroute utility displays the route used by IP packets on their way to a specified network (or Internet) host. Traceroute displays the IP number and host name (if possible) of the machines along the route taken by the packets. Traceroute is used as a network debugging tool. If you're having network connectivity problems, traceroute will show you where the trouble is coming from along the route. Install traceroute if you need a tool for diagnosing network connectivity problems.
- 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-2010l-1.el5 - tzdata-2011g-1.el5

- Group: System Environment/Base
- Summary: Timezone data

- Description: This package contains data files with rules for various time zones 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

udev-095-14.24.el5 - udev-095-14.27.el5

- Group: System Environment/Base
- Summary: A userspace implementation of devfs
- Description: The udev package contains an implementation of devfs in userspace using sysfs and netlink.
- 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-3.5.0-1.el5 - valgrind-3.5.0-5.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

virt-manager-0.6.1-13.el5 - virt-manager-0.6.1-14.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
- No added obsoletes
- No removed obsoletes

vnc-4.1.2-14.el5_5.4 - vnc-4.1.2-14.el5_6.6

- Group: User Interface/Desktops
- Summary: A remote display system.
- Description: Virtual Network Computing (VNC) is a remote display system 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. This package contains a client which will allow you to connect to other desktops running a VNC 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

vsftpd-2.0.5-16.el5_5.1 - vsftpd-2.0.5-21.el5

- 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

w3m-0.5.1-17.el5_5 - w3m-0.5.1-18.el5

- Group: Applications/Internet
- Summary: A pager with Web browsing abilities.
- Description: The w3m program is a pager (or text file viewer) that can also be used as a text-mode Web browser. W3m features include the following: when reading an HTML document, you can follow links and view images using an external image viewer; its internet message mode determines the type of document from the header; if the Content-Type field of the document is text/html, the document is displayed as an HTML document; you can change a URL description like 'http://hogege.net' in plain text into a link to that URL. If you want to display the inline images on w3m, you need to install w3m-img package as well.
- 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-0.14-7 - wdaemon-0.14-8

- 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

wireshark-1.0.15-1.el5_5.1 - wireshark-1.0.15-1.el5_6.4

- Group: Applications/Internet
- Summary: Network traffic analyzer
- Description: Wireshark is a network traffic analyzer for Unix-ish operating systems. This package lays base for libpcap, a packet capture and filtering library, contains command-line utilities, contains plugins and documentation for wireshark. A graphical user interface is packaged separately to GTK+ 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

xen-3.0.3-120.el5 - xen-3.0.3-132.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.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xinetd-2.3.14-10.el5 - xinetd-2.3.14-13.el5

- Group: System Environment/Daemons
- Summary: A secure replacement for inetd.
- Description: Xinetd is a secure replacement for inetd, the Internet services daemon. Xinetd provides access control for all services based on the address of the remote host and/or on time of access and can prevent denial-of-access attacks. Xinetd provides extensive logging, has no limit on the number of server arguments, and lets you bind specific services to specific IP addresses on your host machine. Each service has its own specific configuration file for Xinetd; the files are located in the /etc/xinetd.d directory.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xmlsec1-1.2.9-8.1.1 - xmlsec1-1.2.9-8.1.2

- 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-drv-ati-6.6.3-3.32.el5 - xorg-x11-drv-ati-6.6.3-3.33.el5

- Group: User Interface/X Hardware Support
- Summary: Xorg X11 ati video driver
- Description: X.Org X11 ati 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-mga-1.4.13-1.el5 - xorg-x11-drv-mga-1.4.13-2.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-qxl-0.0.12-1.2.el5 - xorg-x11-drv-qxl-0.0.12-2.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-1.3.0-8.2.el5 - xorg-x11-drv-vesa-1.3.0-8.3.el5

- Group: User Interface/X Hardware Support
- Summary: Xorg X11 vesa video driver
- Description: X.Org X11 vesa video driver.
- Added Dependencies:
  - xorg-x11-server-sdk >= 1.1.1-48.22
- Removed Dependencies:
  - xorg-x11-server-sdk >= 1.1.0-1
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xorg-x11-font-utils-7.1-2 - xorg-x11-font-utils-7.1-3

- Group: User Interface/X
- Summary: X.Org X11 font utilities
- Description: X.Org X11 font utilities required for font installation, conversion, and generation.
- 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-1.1.1-48.76.el5_5.2 - xorg-x11-server-1.1.1-48.76.el5_6.4

- Group: User Interface/X
- Summary: X.Org X11 X server
- Description: X.Org X11 X 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

xorg-x11-server-utils-7.1-4.fc6 - xorg-x11-server-utils-7.1-5.el5_6.2

- Group: User Interface/X
- Summary: X.Org X11 X server utilities
- Description: A collection of utilities used to tweak and query the runtime configuration of the X 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

xorg-x11-xfs-1.0.2-4 - xorg-x11-xfs-1.0.2-5.el5_6.1

- Group: System Environment/Daemons
- Summary: X.Org X11 xfs font server
- Description: X.Org X11 xfs font 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

xulrunner-1.9.2.13-3.el5 - xulrunner-1.9.2.18-2.el5_6

- Group: Applications/Internet
- Summary: XUL Runtime for Gecko Applications
- Description: XULRunner provides the XUL Runtime environment for Gecko 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

yaboot-1.3.13-10.el5_5.1 - yaboot-1.3.13-12.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

ypbind-1.19-12.el5 - ypbind-1.19-12.el5_6.1

- Group: System Environment/Daemons
- Summary: The NIS daemon which binds NIS clients to an NIS domain.
- Description: The Network Information Service (NIS) is a system that provides network information (login names, passwords, home directories, group information) to all of the machines on a network. NIS can allow users to log in 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 provides the ypbind daemon. The ypbind daemon binds NIS clients to an NIS domain. Ypbind must be running on any machines running NIS client programs. Install the ypbind package on any machines running NIS client programs (included in the yp-tools package). If you need an NIS server, you also need to install the ypserv package to a machine 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

ypserv-2.19-5.el5 - ypserv-2.19-5.el5_6.1

- Group: System Environment/Daemons
- Summary: The NIS (Network Information Service) server.
- Description: The Network Information Service (NIS) is a system that provides network information (login names, passwords, home directories, group information) to all of the machines on a network. NIS can allow users to log in 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 provides the NIS server, which will need to be running on your network. NIS clients do not need to be running the server. Install ypserv if you need an NIS server for your network. You also need to install the yp-tools and ypbind packages on any NIS client 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

yum-3.2.22-33.el5 - yum-3.2.22-37.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-0.5.4-17.el5 - yum-rhn-plugin-0.5.4-22.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

yum-utils-1.1.16-13.el5_4.1 - yum-utils-1.1.16-16.el5

- Group: Development/Tools
- Summary: Utilities based around the yum package manager
- Description: yum-utils is a collection of utilities and examples for the yum package manager. It includes utilities by different authors that make yum easier and more powerful to use. These tools include: debuginfo-install, package-cleanup, repoclosure, repodiff, repo-graph, repomanage, repoquery, repo-rss, reposync, repotrack, verifytree, yum-builddep, yum-complete-transaction, yumdownloader, yum-debug-dump and yum-groups-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

zlib-1.2.3-3 - zlib-1.2.3-4.el5

- Group: System Environment/Libraries
- Summary: The zlib compression and decompression library.
- Description: Zlib is a general-purpose, patent-free, lossless data compression library which is used by many different 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

APPENDIX B. REVISION HISTORY

Revision 0-27.402 **Fri Oct 25 2013** **Rüdiger Landmann**

Rebuild with Publican 4.0.0

Revision 0-27 **Mon Jun 4 2012** **Martin Prpič**

Fixed Stateless Linux description and removed outdated reference to Fedora page.

Revision 0-1 **Thu Jul 21 2011** **Martin Prpič**

Release of the Red Hat Enterprise Linux 5.7 Technical Notes

Revision 0-0 **Tue Nov 30 2010** **Ryan Lerch**

Initial release of the Technical Notes