Red Hat Enterprise Linux 6
6.7 Technical Notes

Detailed notes on the changes implemented in Red Hat Enterprise Linux 6.7
Edition 7

Red Hat Customer Content Services

Red Hat Enterprise Linux 6 6.7 Technical Notes

Detailed notes on the changes implemented in Red Hat Enterprise Linux 6.7
Edition 7

Red Hat Customer Content Services

Legal Notice

Abstract

The Red Hat Enterprise Linux 6.7 Technical Notes list and document the changes made to the Red Hat Enterprise Linux 6 operating system and its accompanying applications between Red Hat Enterprise Linux 6.6 and minor release Red Hat Enterprise Linux 6.7.

Table of Contents

Preface

The *Red Hat Enterprise Linux 6.7 Technical Notes* list and document the changes made to the Red Hat Enterprise Linux 6 operating system and its accompanying applications between minor release Red Hat Enterprise Linux 6.6 and minor release Red Hat Enterprise Linux 6.7.

For system administrators and others planning Red Hat Enterprise Linux 6.7 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 6.7 Technical Notes* provide a single, organized source for change tracking and compliance testing.

For every user, the *Red Hat Enterprise Linux 6.7 Technical Notes* provide details of what has changed in this new release.

Note

The Package Manifest is available as a separate document.

Chapter 1. Red Hat Enterprise Linux 6.7 International Languages

Red Hat Enterprise Linux 6.7 supports installation of multiple languages and changing of languages based on your requirements.

The following languages are supported in Red Hat Enterprise Linux 6.7:

- East Asian Languages - Japanese, Korean, Simplified Chinese, and Traditional Chinese
- European Languages - English, German, Spanish, French, Portuguese Brazilian, and Russian,
- Indic Languages - Assamese, Bengali, Gujarati, Hindi, Kannada, Malayalam, Marathi, Oriya, Punjabi, Tamil, and Telugu

The table below summarizes the currently supported languages, their locales, default fonts installed and packages required for some of the supported languages

Table 1.1. Red Hat Enterprise Linux 6 International Languages

Territory	Language	Locale	Fonts	Package Names
China	Simplified Chinese	zh_CN.UTF-8	AR PL (ShanHeiSun and Zenkai) Uni	fonts-chinese, scim-pinyin, scim-tables
Japan	Japanese	ja_JP.UTF-8	Sazanami (Gothic and Mincho)	fonts-japanese, scim-anthy
Korea	Hangul	ko_KR.UTF-8	Baekmuk (Batang, Dotum, Gulim, Headline)	fonts-korean, scim-hangul
Taiwan	Traditional Chinese	zh_TW.UTF-8	AR PL (ShanHeiSun and Zenkai) Uni	fonts-chinese, scim-chewing, scim-tables
Brazil	Portuguese	pt_BR.UTF-8	standard latin fonts	
France	French	ft_FR.UTF-8	standard latin fonts	
Germany	German	de_DE.UTF-8	standard latin fonts	
Italy	Italy	it_IT.UTF-8	standard latin fonts	
Russia	Russian	ru_RU.UTF-8	KOI8-R, fonts-KOI8-R-100dpi, fonts-KOI8-R-75dpi and xorg-x11-fonts-cyrillic	fonts-KO18-R, fonts-KO18-R-100dpi,fonts-KO18-R-75dpi, xorg-x11-fonts-cyrillic
Spain	Spanish	es_ES.UTF-8	standard latin fonts	
India	Assamese	as_IN.UTF-8	Lohit Bengali	fonts-bengali, scim-m17n, m17n-db-assamese
	Bengali	bn_IN.UTF-8	Lohit Bengali	fonts-bengali, scim-m17n, m17n-db-bengali

Territory	Language	Locale	Fonts	Package Names
	Gujarati	gu_IN.UTF-8	Lohit Gujarati	fonts-gujarati, scim-m17n, m17n-db-gujarati
	Hindi	hi_IN.UTF-8	Lohit Hindi	fonts-hindi, scim-m17n, m17n-db-hindi
	Kannada	kn_IN.UTF-8	Lohit Kannada	fonts-kannada, scim-m17n, m17n-db-kannada
	Malayalam	ml_IN.UTF-8	Lohit Malayalam	fonts-malayalam, scim-m17n, m17n-db-malayalam
	Marathi	mr_IN.UTF-8	Lohit Hindi	fonts-hindi, scim-m17n, m17n-db-marathi
	Oriya	or_IN.UTF-8	Lohit Oriya	fonts-oriya, scim-m17n, m17n-db-oriya
	Punjabi	pa_IN.UTF-8	Lohit Punjabi	fonts-punjabi, scim-m17n, m17n-db-punjabi
	Tamil	ta_IN.UTF-8	Lohit Tamil	fonts-tamil, scim-m17n, m17n-db-tamil
	Telugu	te_IN.UTF-8	Lohit Telugu	fonts-telugu, scim-m17n, m17n-db-telugu

Chapter 2. Important Changes to External Kernel Parameters

This chapter provides system administrators with a summary of significant changes in the kernel shipped with Red Hat Enterprise Linux 6.7. These changes include added or updated **procfs** entries, **sysfs** default values, boot parameters, kernel configuration options, or any noticeable behavior changes.

efi_smbios_addr [X86,EFI]

Parameter used to specify location of SMBIOS for EFI systems. Used by *kexec-tools* for *kdump*.

initcall_blacklist [KNL]

A comma-separated list of initcall functions that should not be executed. Useful for debugging built-in modules and initcalls.

panic_on_warn

When enabled (set to **1**), panic() is called after printing out the WARN() location. This is useful when you want to cause kdump on WARN().

/proc/<pid>/numa_maps

Shows memory location, binding policy, and mapping details of each mapping. Mapping details now include the page size in kilobytes (***kernelpagesize_kB***), in addition to mapping type, page usage counters, and node-based page counters.

/proc/<pid>/smaps

Shows memory consumption for each mapping of a process. The output now includes the kernel flags associated with the particular area of virtual memory (***VmFlags***). Kernel flags are shown as a space-separated list of two-letter codes:

Table 2.1. VmFlags Codes

Code	Description
rd	readable
wr	writeable
ex	executable
sh	shared
mr	may read
mw	may write
me	may execute
ms	may share
gd	stack segment grows down
pf	pure PFN range
dw	disabled write to the mapped file
lo	pages are locked in memory
io	memory mapped I/O area
sr	sequential read advise provided
rr	random read advise provided
dc	do not copy area on fork
de	do not expand area on remapping
ac	area is accountable

Code	Description
nr	swap space is not reserved for the area
ht	area uses huge tlb pages
nl	non-linear mapping
ar	architecture specific flag
dd	do not include area into core dump
mm	mixed map area
hg	huge page advise flag
nh	no-huge page advise flag
mg	mergable advise flag

net.ip.ip_no_pmtu_disc

Disables Path MTU Discovery. This parameter was previously Boolean; it now takes an Integer as a value. Possible values include:

0 (default)

Enables Path MTU Discovery.

1

Disables Path MTU Discovery by setting the PMTU to this destination to the value of ***min_pmtu*** when a fragmentation-requiring ICMP is received. To avoid locally-generated fragments, manually increase the value of ***min_pmtu*** to the interface on your system that has the smallest MTU.

2

Disables Path MTU Discovery by discarding Path MTU discovery messages. Outgoing frames are handled in the same way as in mode **1**, implicitly setting ***IP_PMTUDISC_DONT*** on every created socket.

net.ip.ip_forward_use_pmtu

Disabled (set to **0**) by default. When enabled, allows Path MTU Discovery while forwarding. Only enable this if you have user space software that depends on the kernel honoring Path MTU Discovery information.

net.core.netdev_rss_key

Contains a randomly generated host key used by drivers that enable RSS (Receive Side Scaling). Most drivers use 40 byte keys; this parameter allows keys up to 52 bytes. If no driver has ever called netdev_rss_key_fill(), this file contains null bytes.

vm.admin_reserve_kbytes

Defines the amount of free memory that should be reserved for users with the **cap_sys_admin** capability. On x86_64, the default value is 8 MB. This is sufficient when using the default overcommit mode. However, on systems where overcommit is set to **never**, this should be increased to account for the full size of recovery programs in virtual memory. On x86_64, the minimum useful reserve is about 128 MB. Changes to this parameter take effect whenever an application requests memory.

Chapter 3. Device Drivers

This chapter provides a comprehensive listing of all device drivers which were updated in Red Hat Enterprise Linux 6.7.

Storage Drivers

- The **hpsa** driver has been upgraded to version 3.4.4-1-RH4.
- The **lpfc** driver has been upgraded to version 10.6.0.20.
- The **megaraid_sas** driver has been upgraded to version 06.806.08.00-rh3.
- The **mpt2sas** driver has been upgraded to version 20.101.00.00.
- The **mpt3sas** driver has been upgraded to version 04.100.00.00-rh.
- The **Multiple Devices (MD)** drivers have been upgraded to the latest upstream version.
- The **Nonvolatile Memory Express (NVMe)** driver has been upgraded to version 0.10.
- The **qla4xxx** driver has been upgraded to version 5.03.00.00.06.07-k0.
- The **qla2xxx** driver has been upgraded to version 8.07.00.16.06.7-k.

Network Drivers

- The **be2net** driver has been upgraded to version 10.4r.
- The **cnic** driver has been upgraded to version 2.5.20.
- The **bonding** driver has been upgraded to version 3.7.1.
- The **forcedeth** driver has been upgraded to the latest upstream version.
- The **i40e** driver has been upgraded to version 1.2.9-k.
- The **qlcnic** driver has been upgraded to version 5.3.62.1.
- The **r8169** driver has been upgraded to version 2.3LK-NAPI.

Miscellaneous Drivers

- The **drm** driver has been upgraded to the latest upstream version.
- The **scsi_debug** driver has been updated to version 1.82.

Chapter 4. Technology Previews

This chapter provides a list of all available Technology Previews in Red Hat Enterprise Linux 6.7.

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. Errata 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 clustering to fully support Technology Preview features in a future release.

4.1. Storage and File Systems

dm-era Device Mapper

The *device-mapper-persistent-data* package now provides tools to help use the new **dm-era** device mapper functionality released as a Technology Preview. The **dm-era** functionality keeps track of which blocks on a device were written within user-defined periods of time called an **era**. This functionality allows backup software to track changed blocks or restore the coherency of a cache after reverting changes.

dm-cache device-mapper Target

The **dm-cache** device-mapper target, which allows fast storage devices to act as a cache for slower storage devices, has been added as a Technology Preview. See the *lvmcache* manual page for more information.

Cross Realm Kerberos Trust Functionality for samba4 Libraries

The Cross Realm Kerberos Trust functionality provided by Identity Management, which relies on the capabilities of the samba4 client library, is included as a Technology Preview starting with Red Hat Enterprise Linux 6.4. This functionality uses the libndr-nbt library to prepare Connection-less Lightweight Directory Access Protocol (CLDAP) messages.

Package: *samba-3.6.23-20*

System Information Gatherer and Reporter (SIGAR)

The System Information Gatherer and Reporter (SIGAR) is a library and command-line tool for accessing operating system and hardware level information across multiple platforms and programming languages. In Red Hat Enterprise Linux 6.4 and later, SIGAR is considered a Technology Preview package.

Package: *sigar-1.6.5-0.4.git58097d9*

DIF/DIX support

DIF/DIX, is a new addition to the SCSI Standard and a Technology Preview in Red Hat Enterprise Linux 6. DIF/DIX increases the size of the commonly used 512-byte disk block from 512 to 520 bytes, adding the Data Integrity Field (DIF). The DIF stores a checksum value for the data block that is calculated by the Host Bus Adapter (HBA) when a write occurs. The storage device then confirms the checksum on receive, and stores both the

data and the checksum. Conversely, when a read occurs, the checksum can be checked by the storage device, and by the receiving HBA.

The DIF/DIX hardware checksum feature must only be used with applications that exclusively issue ***O_DIRECT*** I/O. These applications may use the raw block device, or the XFS file system in ***O_DIRECT*** mode. (XFS is the only file system that does not fall back to buffered I/O when doing certain allocation operations.) Only applications designed for use with ***O_DIRECT*** I/O and DIF/DIX hardware should enable this feature.

For more information, refer to section *Block Devices with DIF/DIX Enabled* in the Storage Administration Guide.

Package: *kernel-2.6.32-554*

Btrfs, BZ#614121

Btrfs is under development as a file system capable of addressing and managing more files, larger files, and larger volumes than the ext2, ext3, and ext4 file systems. Btrfs is designed to make the file system tolerant of errors, and to facilitate the detection and repair of errors when they occur. It uses checksums to ensure the validity of data and metadata, and maintains snapshots of the file system that can be used for backup or repair. The Btrfs Technology Preview is only available on AMD64 and Intel 64 architectures.

Btrfs is still experimental

Red Hat Enterprise Linux 6 includes Btrfs as a technology preview to allow you to experiment with this file system. You should not choose Btrfs for partitions that will contain valuable data or that are essential for the operation of important systems.

Package: *btrfs-progs-0.20-0.2.git91d9eec*

LVM Application Programming Interface (API)

Red Hat Enterprise Linux 6 features the new LVM application programming interface (API) as a Technology Preview. This API is used to query and control certain aspects of LVM.

Package: *lvm2-2.02.118-2*

FS-Cache

FS-Cache in Red Hat Enterprise Linux 6 enables networked file systems (for example, NFS) to have a persistent cache of data on the client machine.

Package: *cachefilesd-0.10.2-1*

eCryptfs File System

eCryptfs is a stacked, cryptographic file system. It is transparent to the underlying file system and provides per-file granularity. eCryptfs is provided as a Technology Preview in Red Hat Enterprise Linux 6.

Package: *ecryptfs-utils-82-6*

4.2. Networking

Mellanox SR-IOV Support

Single Root I/O Virtualization (SR-IOV) is now supported as a Technology Preview in the Mellanox **libmlx4** library and the following drivers:

- **mlx_core**
- **mlx4_ib** (InfiniBand protocol)
- **mlx_en** (Ethernet protocol)

Package: *kernel-2.6.32-554*

Open multicast ping (Omping), BZ#657370

Open Multicast Ping (Omping) is a tool to test the IP multicast functionality, primarily in the local network. This utility allows users to test IP multicast functionality and assists in the diagnosing if an issues is in the network configuration or elsewhere (that is, a bug). In Red Hat Enterprise Linux 6 Omping is provided as a Technology Preview.

Package: *omping-0.0.4-1*

QFQ queuing discipline

In Red Hat Enterprise Linux 6, the **tc** utility has been updated to work with the Quick Fair Scheduler (QFQ) kernel features. Users can now take advantage of the new QFQ traffic queuing discipline from userspace. This feature is considered a Technology Preview.

Package: *kernel-2.6.32-554*

vios-proxy, BZ#721119

vios-proxy is a stream-socket proxy for providing connectivity between a client on a virtual guest and a server on a Hypervisor host. Communication occurs over virtio-serial links.

Package: *vios-proxy-0.2-1*

4.3. Clustering and High Availability

luci support for fence_sanlock

The **luci** tool now supports the sanlock fence agent as a Technology Preview. The agent is available in the luci's list of agents.

Package: *luci-0.26.0-67*

Recovering a node via a hardware watchdog device

New fence_sanlock agent and checkquorum.wdmd, included in Red Hat Enterprise Linux 6.4 as a Technology Preview, provide new mechanisms to trigger the recovery of a node via a hardware watchdog device. Tutorials on how to enable this Technology Preview will be available at https://fedorahosted.org/cluster/wiki/HomePage

Note that SELinux in enforcing mode is currently not supported.

Package: *cluster-3.0.12.1-73*

4.4. Authentication

Apache Modules for External Authentication

A set of Apache modules has been added to Red Hat Enterprise Linux 6.6 as a Technology Preview. The **mod_authnz_pam**, **mod_intercept_form_submit**, and **mod_lookup_identity** Apache modules in the respective packages can be used by Web applications to achieve tighter interaction with external authentication and identity sources, such as Identity Management in Red Hat Enterprise Linux.

Simultaneous maintaining of TGTs for multiple KDCs

Kerberos version 1.10 added a new cache storage type, DIR:, which allows Kerberos to maintain Ticket Granting Tickets (TGTs) for multiple Key Distribution Centers (KDCs) simultaneously and auto-select between them when negotiating with Kerberized resources. Red Hat Enterprise Linux 6.4 and later includes SSSD enhanced to allow the users to select the DIR: cache for users that are logging in via SSSD. This feature is introduced as a Technology Preview.

Package: *sssd-1.12.4-31*

4.5. Security

TPM

TPM (Trusted Platform Module) hardware can create, store and use RSA keys securely (without ever being exposed in memory), verify a platform's software state using cryptographic hashes and more. The *trousers* and *tpm-tools* packages are considered a Technology Preview.

Packages: *trousers-0.3.13.2*, *tpm-tools-1.3.4-2*

4.6. Devices

mpt2sas lockless mode

The **mpt2sas** driver is fully supported. However, when used in the lockless mode, the driver is a Technology Preview.

Package: *kernel-2.6.32-554*

4.7. Kernel

Kernel Media support

The following features are presented as Technology Previews:

- The latest upstream video4linux
- Digital video broadcasting
- Primarily infrared remote control device support
- Various webcam support fixes and improvements

Package: *kernel-2.6.32-554*

Linux (NameSpace) Container [LXC]

Linux containers provide a flexible approach to application runtime containment on bare-metal systems without the need to fully virtualize the workload. Red Hat Enterprise Linux 6

provides application level containers to separate and control the application resource usage policies via cgroups and namespaces. This release includes basic management of container life-cycle by allowing creation, editing and deletion of containers via the **libvirt** API and the **virt-manager** GUI. Linux Containers are a Technology Preview.

Packages: *libvirt-0.10.2-53*, *virt-manager-0.9.0-29*

Diagnostic pulse for the fence_ipmilan agent, BZ#655764

A diagnostic pulse can now be issued on the IPMI interface using the **fence_ipmilan** agent. This new Technology Preview is used to force a kernel dump of a host if the host is configured to do so. Note that this feature is not a substitute for the **off** operation in a production cluster.

Package: *fence-agents-4.0.15-8*

4.8. Virtualization

Red Hat Enterprise Linux 6.6 Hosted as a Generation 2 Virtual Machine

As a Technology Preview, Red Hat Enterprise Linux 6.6 can be used as a generation 2 virtual machine in the Microsoft Hyper-V Server 2012 R2 host. In addition to the functions supported in the previous generation, generation 2 provides new functions on a virtual machine; for example: boot from a SCSI virtual hard disk, and UEFI firmware support.

Chapter 5. Deprecated Functionality

`mingw` component

Following the deprecation of Matahari packages in Red Hat Enterprise Linux 6.3, at which time the *mingw* packages were noted as deprecated, and the subsequent removal of Matahari packages from Red Hat Enterprise Linux 6.4, the *mingw* packages were removed from Red Hat Enterprise Linux 6.6 and later.

The *mingw* packages are no longer shipped in Red Hat Enterprise Linux 6 minor releases, nor will they receive security-related updates. Consequently, users are advised to uninstall any earlier releases of the *mingw* packages from their Red Hat Enterprise Linux 6 systems.

`virtio-win` component, BZ#1001981

The VirtIO SCSI driver has been removed from the virtio-win package and is no longer supported on Microsoft Windows Server 2003 platform.

`qemu-kvm` component

The *qemu-guest-agent-win32* package is no longer shipped as part of the *qemu-kvm* package. The Windows guest agent is now delivered in the Supplementary channel together with other Windows components, for example, *virtio-win* drivers.

`fence-agents` component

Prior to Red Hat Enterprise Linux 6.5 release, the Red Hat Enterprise Linux High Availability Add-On was considered fully supported on certain VMware ESXi/vCenter versions in combination with the fence_scsi fence agent. Due to limitations in these VMware platforms in the area of SCSI-3 persistent reservations, the **`fence_scsi`** fencing agent is no longer supported on any version of the Red Hat Enterprise Linux High Availability Add-On in VMware virtual machines, except when using iSCSI-based storage. See the Virtualization Support Matrix for High Availability for full details on supported combinations:

https://access.redhat.com/site/articles/29440

Users using **`fence_scsi`** on an affected combination can contact Red Hat Global Support Services for assistance in evaluating alternative configurations or for additional information.

`matahari` component

The **Matahari** agent framework (*matahari-**) packages have been removed from Red Hat Enterprise Linux 6. Focus for remote systems management has shifted towards the use of the CIM infrastructure. This infrastructure relies on an already existing standard which provides a greater degree of interoperability for all users.

`distribution` component

The following packages have been deprecated and are subjected to removal in a future release of Red Hat Enterprise Linux 6. These packages will not be updated in the Red Hat Enterprise Linux 6 repositories and customers who do not use the MRG-Messaging product are advised to uninstall them from their system.

- *python-qmf*
- *python-qpid*
- *qpid-cpp*

- *qpid-qmf*
- *qpid-tests*
- *qpid-tools*
- *ruby-qpid*
- *saslwrapper*

Red Hat MRG-Messaging customers will continue to receive updated functionality as part of their regular updates to the product.

`fence-virt` component

The **libvirt-qpid** is no longer part of the fence-virt package.

openscap component

The *openscap-perl* subpackage has been removed from *openscap*.

Chapter 6. New Packages

6.1. RHEA-2015:1420 — new packages: clufter

New clufter packages are now available for Red Hat Enterprise Linux 6.

The clufter packages contain a tool for transforming and analyzing cluster configuration formats. Notably, clufter can be used to assist with migration from an older stack configuration to a newer one that leverages Pacemaker. The packages can be used either as a separate command-line tool or as a Python library.

This enhancement update adds the clufter packages to Red Hat Enterprise Linux 6. (BZ#1182358)

All users who require clufter are advised to install these new packages.

6.2. RHEA-2015:1354 — new packages: lshw

New lshw packages are now available for Red Hat Enterprise Linux 6.

The lshw packages include a utility that provides detailed information on the hardware configuration of a machine. It reports, for example, information about memory configuration, firmware version, motherboard configuration, CPU version and speed, cache configuration, and bus speed.

All users who require lshw are advised to install these new packages.

6.3. RHEA-2015:1414 — new package: python-argparse

A new python-argparse package is now available for Red Hat Enterprise Linux 6.

The python-argparse package provides the argparse module, which is an improved version of the optparse command-line parser.

This enhancement update adds the python-argparse package to Red Hat Enterprise Linux 6. The package is now available from the base channels in Red Hat Network. (BZ#1173360)

All users who require python-argparse are advised to install this new package.

6.4. RHEA-2015:1418 — new packages: python-requests and dependencies

A new python-requests package and its dependencies, python-chardet, python-urllib3, python-six, python-backports, and python-backports-ssl_match_hostname, are now available for Red Hat Enterprise Linux 6.

The python-requests package contains a library designed to make HTTP requests easy for developers.

This enhancement update adds the python-requests package and its dependencies to Red Hat Enterprise Linux 6. The following packages are now available from the base channels in Red Hat Network: python-requests, python-chardet, python-urllib3, python-six, python-backports, and python-backports-ssl_match_hostname. (BZ#1176248, BZ#1176251, BZ#1176257, BZ#1176258, BZ#1183141, BZ#1183146)

All users who require python-requests, python-chardet, python-urllib3, python-six, python-backports, and python-backports-ssl_match_hostname are advised to install these new packages.

6.5. RHEA-2015:1421 — new package: redhat-access-insights

A new redhat-access-insights package is now available for Red Hat Enterprise Linux 6.

The redhat-access-insights package allows Red Hat subscribers to enroll in a powerful analytics toolchain that allows them to proactively discover and triage problems that have been detected in their Red Hat Enterprise Linux. The information and schedule for analysis upload can be set by the user.

This enhancement update adds the redhat-access-insights package to Red Hat Enterprise Linux 6. (BZ#1176237)

All users who require redhat-access-insights are advised to install this new package.

6.6. RHEA-2015:1364 — new packages: scap-workbench

New scap-workbench packages are now available for Red Hat Enterprise Linux 6.

The scap-workbench packages provide a GUI utility for scanning Security Content Automation Protocol (SCAP) content.

This enhancement update adds the scap-workbench packages to Red Hat Enterprise Linux 6. (BZ#1152954)

All users who require scap-workbench are advised to install these new packages.

Chapter 7. Updated Packages

7.1. 389-ds-base

7.1.1. RHBA-2015:1326 — 389-ds-base bug fix and enhancement update

Updated 389-ds-base packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The 389 Directory Server is an LDAPv3 compliant server. The base packages include the LDAP server and command-line utilities for server administration.

Bug Fixes

BZ#1193243

When a suffix-mapping tree entry was created without the corresponding back-end database, the server failed to start. This bug has been fixed.

BZ#1145072

If a value of a password policy attribute was deleted, it caused a null reference and an unexpected termination of the server. These crashes no longer occur.

BZ#1080185, BZ#1138745

This update fixes a memory leak caused by a previous patch for BZ#1080185.

BZ#1048987

If a Virtual List View search fails with the timelimit or adminlimit parameters exceeded, the allocated memory of the IDL no longer leaks.

BZ#1162704

If a search for "passwordAdminDN" in a "cn=config" entry returns a non-existing value, a memory leak no longer occurs.

BZ#1169975

Rebuilding the Class of Service (CoS) cache no longer causes a memory leak.

BZ#1115960

A bug in the nested CoS, when the closest above password policy was sometimes not selected as expected, has been fixed.

BZ#1169974

When a SASL bind operation fails and Account Lockout is enabled, the Root DSE entry no longer gets incorrectly updated with passwordRetryCount.

BZ#1145379

Password restrictions and syntax checks for Directory Manager and password administrators are now properly applied so that these roles are not affected by them.

BZ#1175868, BZ#1166313

Performance degradation with searches in large groups has been fixed by introducing normalized DN cache.

BZ#1153739

Due to a known vulnerability in SSLv3, this protocol is now disabled by default.

BZ#1207024

This update adds the flow control so that unbalanced process speed between a supplier and a consumer does not cause replication to become unresponsive.

BZ#1171308

A bug to replicate an "add: userPassword" operation has been fixed.

BZ#1145374, BZ#1183820

A bug in the Windows Sync plug-in code caused AD-only member values to be accidentally removed. Now, local and remote entries are handled properly, preventing data loss.

BZ#1144092

Performing a schema reload sometimes caused a running search to fail to return results. Now, the old schema is not removed until the reload is complete. The search results are no longer corrupted.

BZ#1203338

The Berkeley DB library terminated unexpectedly when the Directory Server simultaneously opened an index file and performed a search on the "cn=monitor" subtree. The two operations are now mutually exclusive, which prevents the crash.

BZ#1223068, BZ#1228402

When simple paged results requests were sent to the Directory Server asynchronously and then abandoned immediately, the search results could leak. Also, the implementation of simple paged results was not thread-safe. This update fixes the leak and modifies the code to be thread-safe.

Enhancements

BZ#1167976

A new memberOf plug-in configuration attribute memberOfSkipNested has been added. This attribute allows you to skip the nested group check, which improves performance of delete operations.

BZ#1118285

The Directory Server now supports TLS versions supported by the NSS library.

BZ#1193241

The logconv.pl utility has been updated to include information about the SSL/TLS versions in the access log.

Users of 389-ds-base are advised to upgrade to these updated packages, which fix these bugs and add these enhancements. After installing this update, the 389 server service will be restarted automatically.

7.2. ImageMagick

7.2.1. RHBA-2015:1359 — ImageMagick bug fix and enhancement update

Updated ImageMagick packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

ImageMagick is an image display and manipulation tool for the X Window System that can read and write multiple image formats.

Upgrade to an upstream version

The ImageMagick packages have been upgraded to upstream version 6.7.2.7, which provides a number of bug fixes and enhancements over the previous version. Notably, it addresses a problem with conversion of Portable Network Graphics (PNG) images that caused the size of the converted file to be much larger than that of the original file. (BZ#1158865)

Users of ImageMagick are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.3. NetworkManager

7.3.1. RHBA-2015:1257 — NetworkManager bug fix and enhancement update

Updated NetworkManager packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

NetworkManager is a system network service that manages network devices and connections, attempting to keep active network connectivity when available. Its capabilities include managing Ethernet, wireless, mobile broadband (WWAN), and PPPoE devices, as well as providing VPN integration with a variety of different VPN services.

Bug Fixes

BZ#1181207

NetworkManager could not handle bonding parameters on the kernel command line with Kickstart installations and could terminate unexpectedly. With this update, Kickstart installations succeed.

BZ#1156564

Adding a connection available only to a particular user via nm-connection-editor could result in an incomplete connection being interpreted by the NetworkManager daemon. Applying this unintended configuration caused NetworkManager to terminate unexpectedly. Now, invalid connections are not created, and NetworkManager no longer crashes.

BZ#1173245

Saving Wireless Enterprise connections (802.1X-based) in the editor with the "Available to all users" and "Ask for this password every time" settings created an invalid profile, which disappeared after saving. With this update, nm-connection-editor does not allow saving invalid connections.

BZ#1076169

Previously, NetworkManager sometimes failed to set up DHCPv6, and IPv6 was not configured. With this update, NetworkManager parses RA flags correctly and runs DHCPv6 as intended.

BZ#1085015

This update fixes the translation of the "Create New Ad-Hoc Wireless Network" nm-applet menu entry.

BZ#1003877

Primary bond options were not properly handled in NetworkManager and nm-connection-editor. Now, configurations with active-backup bonds work as intended.

BZ#1157867

Removing an alias ifcfg file made NetworkManager disconnect both the alias and the base interfaces. This has been fixed.

BZ#1167491

When a user mistyped the gateway IP, no warning was provided. Now, nm-connection-editor informs the user of a possibly incorrect gateway field.

BZ#1207599

NetworkManager could sometimes contain duplicated IPv6 addresses in its configuration. With this update, there are no duplicated IPv6 addresses on the D-Bus interface and in the nmcli tool.

BZ#1213327

The nmcli tool could become unresponsive if both NetworkManager and nm-applet were stopped and the "nmcli con" command was issued.

BZ#1111672

Connections with a missing or 0.0.0.0 next-hop address were regarded as invalid.

Enhancements

BZ#979181

Previously, the NM_CONTROLLED=no setting only worked if HWADDR was also set. Now, it is also possible to specify that a device is unmanaged by setting NM_CONTROLLED=no and DEVICE=<interface>.

BZ#1063661

NetworkManager did not allow configuring VLAN on top of bond devices, and Anaconda installations using VLAN over bond did not work. This update adds support for VLANs (IEEE 802.11q) on top of Ethernet Bonds and Ethernet Bridges (IEEE 802.1d).

BZ#905641

This update enhances nm-connection-editor, which now enables easier editing of IP addresses and routes. In addition, nm-connection-editor attempts to automatically detect and highlight typos and incorrect configurations.

BZ#1056790

With this update, NetworkManager supports arping when configuring static IP addresses, so statically configured IPv4 addresses to other nodes on the local network are announced.

BZ#1046074

NetworkManager now supports the "multicast_snooping" option, configured via BRIDGING_OPTS in the ifcfg file, for bridge interfaces.

BZ#1200131

With this update, custom DNS options can be configured in connection profiles. The DNS options are read and written using the RES_OPTIONS variable in ifcfg files.

Users of NetworkManager are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.4. PackageKit

7.4.1. RHBA-2015:1352 — PackageKit bug fix update

Updated PackageKit packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

PackageKit is a D-Bus abstraction layer that allows the session user to manage packages in a secure way using a cross-distribution, cross-architecture API.

Bug Fixes

BZ#1140837

Prior to this update, if the RPM v3 binary was used to re-sign custom and third-party unsigned packages, PackageKit could not handle installing these packages. As a consequence, installing certain packages using the PackageKit GUI could fail with the following error message:

pct = div * (ts_current - 1) + pct_start + ((div / 100.0) * val)

This update fixes PackageKit to handle these rare cases, and the installation no longer fails in the described situation.

BZ#1172119

Previously, when MAILTO recipients were set in the /etc/sysconfig/packagekit-background file, the /etc/cron.daily/packagekit-background.cron script only checked for the return value from the pkcon command before trying to send email reports. As a consequence, two unnecessary empty emails were sent under certain circumstances. With this update, the $PKTMP file is not attempted to be sent by email if the files is empty, and only emails with useful information are now sent in the described scenario.

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

7.5. Red

7.5.1. RHEA-2015:1423 — Red Hat Enterprise Linux 6.7 Release Notes

Updated packages containing the Release Notes for Red Hat Enterprise Linux 6.7 are now available.

Red Hat Enterprise Linux minor releases are an aggregation of individual enhancement, security and bug fix errata. The Red Hat Enterprise Linux 6.7 Release Notes document the major changes made to the Red Hat Enterprise Linux 6 operating system and its accompanying applications for this minor release.

For the most up-to-date version of the Red Hat Enterprise Linux 6.7 Release Notes, see the book online:

https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html-single/6.7_Release_Notes/index.html

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

7.6. SDL

7.6.1. RHBA-2015:0656 — SDL bug fix update

Updated SDL packages that fix one bug are now available for Red Hat Enterprise Linux 6.

Simple DirectMedia Layer (SDL) is a cross-platform multimedia library designed to provide fast access to the graphics frame buffer and audio device.

Bug Fix

BZ#1125304

Due to the changes made to X Virtual Frame Buffer (Xvfb) in Red Hat Enterprise Linux 6.6, the XGrabPointer() function started to return a value of 0 if used on an SDL window placed outside the Xvfb root window boundaries. Consequently, if an SDL program expected the original return value, a problem could occur. With this update, the SDL library conforms to the new behavior, and programs using this library now work as expected.

Users of SDL are advised to upgrade to these updated packages, which fix this bug.

7.6.2. RHBA-2015:1435 — SDL bug fix update

Updated SDL packages that fix one bug are now available for Red Hat Enterprise Linux 6.

Simple DirectMedia Layer (SDL) is a cross-platform multimedia library designed to provide fast access to the graphics frame buffer and audio device.

Bug Fix

BZ#1205603

An attempt to upgrade the SDL library without upgrading the libX11 library could result in applications emitting the following error:

symbol lookup error: /usr/lib64/libSDL-1.2.so.0: undefined symbol: _XGetRequest after updating SDL

This update modifies the SDL spec file to prevent an upgrade on systems with a too outdated libX11 version. As a result, the mentioned error no longer occurs.

Users of SDL are advised to upgrade to these updated packages, which fix this bug.

7.7. abrt

7.7.1. RHBA-2015:1453 — abrt, libreport, and satyr bug fix and enhancement update

Updated abrt, libreport, and satyr packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The Automatic Bug Reporting Tool (ABRT) recognizes defects in applications and creates bug reports that help maintainers to fix the defects. ABRT uses a plug-in system to extend its functionality.

Bug Fixes

BZ#1199261

The abrt-addon-ccpp process logs messages using the rsyslog daemon. When rsyslog terminated unexpectedly, abrt-addon-ccpp could enter a deadlock state, because the /dev/log socket was not freed. The underlying source code has been modified to fix this bug, and the deadlock no longer occurs in the described situation.

BZ#1208154

The "bootloader" plug-in was renamed to "boot". However, ABRT still used the old name when generating SOS reports. As a consequence, ABRT did not include SOS report data in its crash reports. With this update, ABRT now uses the correct name and generates SOS reports as expected.

BZ#1212095

The libreport library could previously change mode of any file or mode of the dump directory because it followed symbolic links. Also, libreport could change ownership of a new dump directory. This behavior could lead to security issues. With this update, this bug has been fixed, and libreport no longer changes modes or ownership.

Enhancement

BZ#1150197, BZ#1152222, BZ#1153311

This update introduces ABRT micro-reporting. When a crash occurs, users can now send authenticated reports about the problem called micro-reports. These reports contain non-sensitive data describing the problem and optionally host name, machine ID, and RHN account number. Micro-reports help Red Hat to track bug occurrences and to provide instant solutions to crashes. See https://access.redhat.com/node/642323 for more information about micro-reporting.

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

7.8. anaconda

7.8.1. RHBA-2015:1297 — anaconda bug fix and enhancement update

Updated anaconda packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The anaconda packages contain portions of the Anaconda installation program that can be run by the user for reconfiguration and advanced installation options.

Bug Fixes

BZ#1145812

On the custom storage screen, selecting mountpoint and format as EFI System Partition caused the following error message to be displayed:

You have not created a /boot/efi partition.

This update modifies the way boot devices are looked up. As a result, an acceptable boot device is located and no error is reported in the described situation.

BZ#1139606

The Anaconda installer set the "boot" flag on the PowerPC Reference Platform (PReP) partition when using GUID Partition Table (GPT) disks. Consequently, the GUID of the partition changed to the EFI System Partition instead of PReP. Now, when using GPT disks, the boot flag is only set on boot partitions that are formatted as EFI partitions, and the PReP partition GUID is no longer replaced with the ESP GUID.

BZ#1153376

The LVM physical volume (PV) and volume group (VG) size was sometimes smaller than expected. Consequently, Anaconda sometimes tried to create a logical volume (LV) that was larger than the available space in the VG. Now, Anaconda verifies the amount of available space when creating a LV and if the request is too large, only the available space is used. Also, a warning message is included in the storage.log file.

BZ#1129499

Under specific circumstances, if a device lookup by name failed, the function failed instead of gracefully returning "no such device". As a consequence, Anaconda terminated unexpectedly. With this update, if a device lookup by name fails, it is treated as if nothing was found instead of an error.

BZ#1083586

Previously, Anaconda forced the vesa driver after the Linux framebuffer (fbdev). As a consquence, the X server could terminate unexpectedly while booting. Now, Anaconda no longer crashes.

BZ#979163

Some servers use network cards that take a very long time to initialize since the link is reported as being available. Consequently, the download of the kickstart file failed. This update re-adds support for the "nicdelay" installer boot option by using NetworkManager's feature of checking the gateway with a ping before the device is reported as connected. As a result, for servers with network cards taking a very long time to initialize, the "nicdelay" boot option can be used to prevent kickstart download from failing.

BZ#1168024

When starting the VNC server, Anaconda always passed the "-nevershared" option, and Anaconda only allowed one VNC connection. This update removes the "-nevershared" option. The user has to use the "-shared" option from their VNC client to connect to a shared connection.

BZ#1021445

The Anaconda installer searched for prepboot disks with a preference for those on the same disk as /boot. If a user deleted all partitions including /boot, the object would be a NoneType. Consequently, Anaconda terminated unexpectedly. This update adds a guard to perform a safe default in the described situation.

Enhancements

BZ#1144979

On IBM System z, if LDL-formatted Direct Access Storage Devices (DASDs) are detected, the Anaconda installer now displays a warning dialog that explains the problem and presents a list of the detected Linux Disk Layout (LDL) DASDs with an option to format them as Compatible Disk Layout (CDL). Before, although LDL DASDs were recognized by the kernel, they were not officially supported in the installer. The user can now choose whether or not to format the detected LDL DASDs as CDL.

BZ#1083459

This update adds support for LVM Thin Provisioning as a device type within the Anaconda installer and kickstart configuration.

Users of anaconda are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.9. at

7.9.1. RHBA-2015:0240 — at bug fix update

Updated at packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The at packages provide a utility for time-oriented job control. The at utility reads commands from standard input or from a specified file and allows you to specify that the commands will be run at a particular time.

Bug Fixes

BZ#994201

Due to incorrect race condition handling in the "atd" daemon, "atd" terminated unexpectedly. With this update, "atd" handles the race condition correctly, so that now "atd" no longer terminates in the described scenario.

BZ#1166882

Previously, the "at" command was not properly checking the return value of the fclose() function call. As a consequence, if the /var/spool/at file system filled up, "at" could leave empty stale files in the spool directory. With this update, "at" properly checks the return value from fclose(), and "at" no longer leaves empty files in spool in the described scenario.

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

7.10. augeas

7.10.1. RHBA-2015:1256 — augeas bug fix and enhancement update

Updated augeas packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

Augeas is a utility for editing configuration. Augeas parses configuration files in their native formats and transforms them into a tree. Configuration changes are made by manipulating this tree and saving it back into native configuration files. Augeas also uses "lenses" as basic building blocks for establishing the mapping from files into the Augeas tree and back.

Bug Fixes

BZ#1112388

Previously, some cgroup controller types used in the /etc/cgconfig.conf file were not recognized. As a consequence, parsing error occurred in Augeas and an error message was returned. With this update, the Augeas module can parse files containing these controller names as expected.

BZ#1121263

Entries in the /etc/services file containing colons in the service name prevented Augeas from parsing the file. This update makes sure that the "service_name" field in the services.aug file is able to support the colon character, and the aforementioned entries can now be parsed successfully.

BZ#1129508

When entries in /etc/rsyslog.conf were configured for remote logging over Transmission Control Protocol (TCP), Augeas was unable to parse the file. The underlying source code has been fixed, and files containing this configuration are now parsed successfully.

BZ#1144652

By default, the /etc/sysconfig/iptables.save file was parsed by the wrong module, which led to a parsing failure and an error reported by Augeas. The wrong module has been substituted with a correct one, and /etc/sysconfig/iptables.save is now parsed correctly by default.

BZ#1175854

Previously, the Augeas utility did not correctly parse the "ssh" and "fence_kdump_*" parameters in the /etc/kdump.conf file. As a consequence, using Augeas to edit these parameters in kdump configuration failed. With this update, Augeas has been updated to parse "ssh" and "fence_kdump_*" as intended, and the described problem no longer occurs.

BZ#1186318

Previously, the aug_match API returned paths of files and nodes with special characters unescaped, unsuitable for use in further API calls. Consequently, specially constructed file names could cause programs built on Augeas to function incorrectly, and implementing escaping in such programs was impossible. With this update, Augeas escapes paths returned from aug_match correctly, and paths returned from aug_match can be used safely and reliably in further API calls.

BZ#1203597

Prior to this update, Augeas was unable to parse the /etc/krb5.conf configuration files containing values with curly brackets ("{}"). To fix this bug, Augeas lens (parser) has been fixed to handle these characters in krb5.conf setting values, and Augeas can now parse these krb5.conf files as expected.

BZ#1209885

Previously. Augeas was unable to parse the .properties (Java-style) files containing a multi-line value that begins with a blank line. Augeas lens (parser) has been fixed to accept an empty starting line, thus fixing this bug.

Enhancement

BZ#1160261

A lens for the /etc/shadow file format has been added to Augeas to parse the shadow password file.

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

7.11. authconfig

7.11.1. RHBA-2015:0760 — authconfig bug fix update

Updated authconfig packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The authconfig packages contain a command line utility and a GUI application that can configure a workstation to be a client for certain network user information and authentication schemes and other user information and authentication related options.

Bug Fixes

BZ#1145137

Prior to this update, it was not possible to specify multiple Lightweight Directory Access Protocol (LDAP) servers with the authconfig command. This bug has been fixed, and multiple LDAP servers can now be specified as expected.

BZ#1194397

Previously, the authconfig utility did not pass passwords provided by the "--winbindjoin" option when calling "net join". Consequently, the user was asked for a password. Now, passwords are passed by authconfig to "net join" automatically, and users do not have to provide them in this situation.

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

7.12. autofs

7.12.1. RHSA-2015:1344 — Moderate: autofs security and bug fix update

Updated autofs packages that fix one security issue and several bugs are now available for Red Hat Enterprise Linux 6.

Red Hat Product Security 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 autofs utility controls the operation of the automount daemon. The daemon automatically mounts file systems when in use and unmounts them when they are not busy.

Security Fix

CVE-2014-8169

It was found that program-based automounter maps that used interpreted languages such as Python would use standard environment variables to locate and load modules of those languages. A local attacker could potentially use this flaw to escalate their privileges on the system.

Note

This issue has been fixed by adding the "AUTOFS_" prefix to the affected environment variables so that they are not used to subvert the system. A configuration option ("force_standard_program_map_env") to override this prefix and to use the environment variables without the prefix has been added. In addition, warnings have been added to the manual page and to the installed configuration file. Now, by default the standard variables of the program map are provided only with the prefix added to its name.

Red Hat would like to thank the Georgia Institute of Technology for reporting this issue.

Bug Fixes

BZ#1163957

If the "ls *" command was executed before a valid mount, the autofs program failed on further mount attempts inside the mount point, whether the mount point was valid or not. While attempting to mount, the "ls *" command of the root directory of an indirect mount was executed, which led to an attempt to mount "*", causing it to be added to the negative map entry cache. This bug has been fixed by checking for and not adding "*" while updating the negative map entry cache.

BZ#1124083

The autofs program by design did not mount host map entries that were duplicate exports in an NFS server export list. The duplicate entries in a multi-mount map entry were recognized as a syntax error and autofs refused to perform mounts when the duplicate entries occurred. Now, autofs has been changed to continue mounting the last seen instance of the duplicate entry rather than fail, and to report the problem in the log files to alert the system administrator.

BZ#1153130

The autofs program did not recognize the yp map type in the master map. This was caused by another change in the master map parser to fix a problem with detecting the map format associated with mapping the type in the master map. The change led to an incorrect length for the type comparison of yp maps that resulted in a match operation failure. This bug has been fixed by correcting the length which is used for the comparison.

BZ#1156387

The autofs program did not update the export list of the Sun-format maps of the network shares exported from an NFS server. This happened due to a change of the Sun-format map parser leading to the hosts map update to stop working on the map re-read operation. The bug has been now fixed by selectively preventing this type of update only for the Sun-formatted maps. The updates of the export list on the Sun-format maps are now visible and refreshing of the export list is no longer supported for the Sun-formatted hosts map.

BZ#1175671

Within changes made for adding of the Sun-format maps, an incorrect check was added that caused a segmentation fault in the Sun-format map parser in certain circumstances. This has been now fixed by analyzing the intent of the incorrect check and changing it in order to properly identify the conditions without causing a fault.

BZ#1201195

A bug in the autofs program map lookup module caused an incorrect map format type comparison. The incorrect comparison affected the Sun-format program maps where it led to the unused macro definitions. The bug in the comparison has been fixed so that the macro definitions are not present for the Sun-format program maps.

Users of autofs are advised to upgrade to these updated packages, which contain backported patches to correct these issues.

7.13. b43-openfwwf

7.13.1. RHBA-2015:1422 — b43-openfwwf bug fix update

An updated b43-openfwwf package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The b43-openfwwf package contains the open firmware for certain Broadcom 43xx series wireless LAN (WLAN) chips. The currently supported models are 4306, 4311 (rev1), 4318, and 4320.

Bug Fix

BZ#1015671

Previously, the b43-openfwwf firmware was incorrectly recognized as the closed-source b43 firmware from Broadcom, which caused the b43 driver to expect the behavior of the Broadcom b43 firmware. This update corrects the location where the firmware images are installed, and as a result, the b43-openfwwf firmware is recognized correctly.

Users of b43-openfwwf are advised to upgrade to this updated package, which fixes this bug.

7.14. bacula

7.14.1. RHBA-2015:0239 — bacula bug fix update

Updated bacula packages that fix one bug are now available for Red Hat Enterprise Linux 6.

Bacula is a set of programs that allow you to manage the backup, recovery, and verification of computer data across a network of different computers.

Bug Fix

BZ#839249

Previously, the length of bacula daemon names was limited to 30 characters and any additional characters were automatically truncated without displaying an error message. The truncated name was passed to other applications that, as a consequence, did not work as expected. With this update, the limit has been exceeded to 64 characters, so the length of the name is no longer cut.

Users of bacula are advised to upgrade to these updated packages, which fix this bug.

7.15. bash

7.15.1. RHBA-2015:1277 — bash bug fix update

Updated bash packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The bash packages provide the Bash (Bourne-again shell) shell, which is the default shell for Red Hat Enterprise Linux.

Bug Fixes

BZ#1148507

Prior to this update, Bash refused to import previously exported functions whose names contained a hyphen. As a consequence, scripts that used such functions did not work properly, and Bash printed the following error message:

bash: error importing function definition for `BASH_FUNC_function-name'

With this update, Bash accepts hyphens in the names of imported functions.

BZ#1150544, BZ#1155455

Previously, Bash incorrectly parsed function definitions containing a here-document that ended with the end-of-file or end-of-string character. Consequently, Bash accessed an invalid memory segment when the parsed function was copied, and Bash terminated with a segmentation fault. This problem has been fixed. As a result, Bash no longer crashes when the aforementioned function definitions are used.

BZ#1119587

The section in the Bash man page describing the ulimit command did not contain the fact that 512-byte blocks are used for the "-c" and "-f" options in POSIX mode. This information has now been added.

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

7.16. bind

7.16.1. RHBA-2015:1250 — bind bug fix and enhancement update

Updated bind packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

BIND (Berkeley Internet Name Domain) is an implementation of the Domain Name System (DNS) 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 correctly.

Bug Fixes

BZ#1112356

Previously, the "slip" option was not handled correctly in the Response Rate Limiting (RRL) code in BIND, and the variable counting the number of queries was not reset after each query, but after every other query. As a consequence, when the "slip" value of the RRL feature was set to one, instead of slipping every query, every other query was dropped. To fix this bug, the RRL code has been amended to reset the variable correctly according to the configuration. Now, when the "slip" value of the RRL feature is set to one, every query is slipped as expected.

BZ#1142152

BIND incorrectly handled errors returned by dynamic databases (from dyndbAPI). Consequently, BIND could enter a deadlock situation on shutdown under certain circumstances. The dyndb API has been fixed not to cause a deadlock during BIND shutdown after the dynamic database returns an error, and BIND now shuts down normally in the described situation.

BZ#1146893

Because the Simplified Database Backend (SDB) application interface did not handle unexpected SDB database driver errors properly, BIND used with SDB could terminate unexpectedly when such errors occurred. With this update, the SDB application interface has been cleaned to handle these errors correctly, and BIND used with SDB no longer crashes if they happen.

BZ#1175321

Due to a race condition in the beginexclusive() function, the BIND DNS server (named) could terminate unexpectedly while loading configuration. To fix this bug, a patch has been applied, and the race condition no longer occurs.

BZ#1215687

Previously, when the resolver was under heavy load, some clients could receive a SERVFAIL response from the server and numerous "out of memory/success" log messages in BIND's log. Also, cached records with low TTL (1) could expire prematurely. Internal hardcoded limits in the resolver have been increased, and conditions for expiring cached records with low TTL (1) have been made stricter. This prevents the resolver from reaching the limits when under heavy load, and the "out of memory/success" log messages from being received. Cached records with low TTL (1) no longer expire prematurely.

Enhancement

BZ#1176476

Users can now use RPZ-NSIP and RPZ-NSDNAME records with Response Policy Zone (RPZ) in the BIND configuration.

Users of BIND are advised to upgrade to these updated packages, which fix these bugs and add this enhancement. After installing the update, the BIND daemon (named) will be restarted automatically.

7.17. bind-dyndb-ldap

7.17.1. RHBA-2015:1259 — bind-dyndb-ldap bug fix update

Updated bind-dyndb-ldap packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The dynamic LDAP back end is a plug-in for BIND that provides back-end capabilities for LDAP databases. It features support for dynamic updates and internal caching that helps to reduce the load on LDAP servers.

Bug Fixes

BZ#1175318

Previously, the bind-dyndb-ldap 2.x driver (used in Red Hat Enterprise Linux 6.x) did not handle forward zones correctly when it was in the same replication topology as bind-dyndb-ldap 6.x (used in Red Hat Enterprise Linux 7.1). As a consequence, forward zones stopped working on all replicas. The underlying source code has been patched to fix this bug, and forward zones now continue to work in the described situation.

BZ#1142176

The bind-dyndb-ldap library incorrectly compared current time and the expiration time of the Kerberos ticket used for authentication to an LDAP server. As a consequence, the Kerberos ticket was not renewed under certain circumstances, which caused the connection to the LDAP server to fail. The connection failure often happened after a BIND service reload was triggered by the logrotate utility. A patch has been applied to fix this bug, and Kerberos tickets are correctly renewed in this scenario.

BZ#1126841

Prior to this update, the bind-dyndb-ldap plug-in incorrectly locked certain data structures. Consequently, a race condition during forwarder address reconfiguration could cause BIND to terminate unexpectedly. This bug has been fixed, bind-dyndb-ldap now locks data structures properly, and BIND no longer crashes in this scenario.

BZ#1219568

Previously, the bind-dyndb-ldap plug-in incorrectly handled timeouts which occurred during LDAP operations. As a consequence, under very specific circumstances, the BIND daemon could terminate unexpectedly. With this update, bind-dyndb-ldap has been fixed to correctly handle timeouts during LDAP operations and the BIND daemon no longer crashes in this scenario.

BZ#1183805

The documentation for bind-dyndb-ldap-2.3 located in the /usr/share/doc/bind-dyndb-ldap-2.3/README file incorrectly stated that the "idnsAllowTransfer" and "idnsAllowQuery" LDAP attributes are multi-valued. Consequently, users were not able to configure DNS zone transfer and query acess control lists according to the documentation. The documentation has been fixed to explain the correct attribute syntax.

Users of bind-dyndb-ldap are advised to upgrade to these updated packages, which fix these bugs.

7.18. binutils

7.18.1. RHBA-2015:1274 — binutils bug fix update

Updated binutils packages that fix one bug are now available for Red Hat Enterprise Linux 6.

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

Bug Fix

BZ#1175590

On IBM System z, the linker sometimes generated undesirable runtime relocations for thread-local-storage variables. These undesirable relocations could under certain circumstances cause execmod AVC errors. This bug has been fixed, and AVC errors are no longer returned in this scenario.

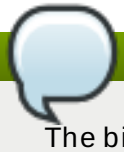
Users of binutils are advised to upgrade to these updated packages, which fix this bug.

7.19. biosdevname

7.19.1. RHBA-2015:1338 — biosdevname bug fix and enhancement update

Updated biosdevname packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The biosdevname packages contain an optional convention for naming network interfaces, which assigns names to network interfaces based on their physical location. The biosdevname utility is disabled by default, except for a limited set of Dell PowerEdge, C Series, and Precision Workstation systems.



Upgrade to an upstream version

The biosdevname packages have been upgraded to upstream version 0.6.2, which provides a number of bug fixes and enhancements over the previous version. Notably, it provides the *dev_port* attribute for a new Mellanox driver and allowing naming of FCoE devices to be ignored. (BZ#1158564)

Bug Fixes

BZ#1133523

Previously, the biosdevname utility did not parse Vital Product Data (VPD) correctly. As a consequence, names for network interfaces on Vindicator 2 Emulex card were displayed incorrectly when NIC extended partitioning (nPAR-EP) was enabled. VPD parsing has been modified, and Network interface names are now displayed correctly.

BZ#1207557

Prior to this update, the biosdevname utility did not read Vital Product Data (VPD) on NICs with vpd-r:2.0, which resulted in incorrect network interface names when NIC partitioning (NPAR) was enabled on certain NICs. With this update, biosdevname reads VPD data also in cases when NIC has vpdr:2.0, and interface names are now formed as expected if NPAR is enabled.

BZ#1212449

Due to a scheme used for slot numbers derivation, the biosdevname utility did not populate proper names for Virtual Functions (VFs) of on-board NICs. Now, the scheme that enables VFs of on-board NICs can have proper names, too.

Enhancements

BZ#1158564

attribute for a new Mellanox driver and allowing naming of FCoE devices to be ignored.

BZ#1003465, BZ#1084225

This update provides an implementation of 10-GB Ethernet adapters naming scheme from Mellanox. Now, the biosdevname utility produces expected network interface names for Mellanox 10-GB Ethernet adapters that have 2 physical ports on the same PCI device. The /sys/class/net/<iface>/dev_port attribute is designed to distinguish network interfaces.

Users of biosdevname are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.20. boost

7.20.1. RHBA-2015:1269 — boost bug update

Updated boost packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The boost packages contain a large number of free peer-reviewed portable C++ source libraries. These libraries are suitable for tasks such as portable file-systems and time/date abstraction, serialization, unit testing, thread creation and multi-process synchronization, parsing, graphing, regular expression manipulation, and many others.

Bug Fixes

BZ#1169501

When compiling a C++ program using the Boost.MPI library, the compiling process previously failed to find the "boost::mpi::environment::environment(bool)" symbol and terminated with an "undefined reference" error. This update adds the missing symbol, and the described compiling process now successfully creates an executable.

BZ#1128313

Previously, the boost packages could use packages for different architectures as their dependencies, which in some cases led to a variety of problems with the functionality of the Boost clients. With this update, dependency declarations specify the architecture of the package where relevant, and all packages necessary for correct operation of the Boost clients are downloaded properly.

BZ#1167383, BZ#1170010

Prior to this update, a number of Boost libraries were not compatible with the GNU Compiler Collection (GCC) provided with Red Hat Developer Toolset. A fix has been implemented to address this problem, and the affected libraries now properly work with Red Hat Developer Toolset GCC.

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

7.21. certmonger

7.21.1. RHBA-2015:1379 — certmonger bug fix and enhancement update

Updated certmonger packages that fix two bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The certmonger service monitors certificates, warns of their impending expiration, and optionally attempts to renew certificates by enrolling the system with a certificate authority (CA).

Bug Fixes

BZ#1163023

Prior to this update, after the user upgraded from Red Hat Enterprise Linux 6.5 to Red Hat Enterprise Linux 6.6 and rebooted the system, certmonger in some cases erroneously exited shortly after starting or performed a series of unnecessary checks for new certificates. A patch has been applied to fix this bug, and these problems no longer occur in the described situation.

BZ#1178190

Previously, the "getcert list" command did not display the "pre-save command" and "post-save command" values. As a consequence, running "getcert list" could return incomplete results. With this update, the problem has been fixed, and running "getcert list" displays the "pre-save command" and "post-save command" values as expected.

Enhancements

BZ#1161768

The certmonger service now supports the Simple Certificate Enrollment Protocol (SCEP). For obtaining certificates from servers, the user can now offer enrollment over SCEP.

BZ#1169806

Requesting a certificate using the getcert utility during an IdM client kickstart enrollment no longer requires certmonger to be running. Previously, an attempt to do this failed because certmonger was not running. With this update, getcert can successfully request a certificate in the described situation, on the condition that the D-Bus daemon is not running. Note that certmonger requires a system reboot to start monitoring the certificate obtained in this way.

BZ#1222595

Previously, after the user ran the "getcert list" command, the output included the PIN value if it was set for the certificate. Consequently, the user could unintentionally expose the PIN, for example by publicly sharing the output of the command. With this update, the "getcert list" output only contains a note that a PIN is set for the certificate. As a result, the PIN value itself is no longer displayed in the "getcert list" output.

Users of certmonger are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.22. chkconfig

7.22.1. RHBA-2015:0671 — chkconfig bug fix update

Updated chkconfig packages that fix one bug are now available for Red Hat Enterprise Linux 6.

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

Bug Fix

BZ#965103

Previously, when the chkconfig utility modified a file in the /etc/xinetd.d/ directory, it set the file permissions to "644" and the SELinux context to "root:object_r:etc_t". Such permissions, however, do not adhere to the Defense Information Systems Agency's (DISA) Security Technical Implementation Guide (STIG), which requires files in /etc/xinetd.d/ to be unreadable by other users. With this update, chkconfig ensures that the xinetd files it modifies have the "600" permissions and the correct SELinux context is preserved.

Users of chkconfig are advised to upgrade to these updated packages, which fix this bug.

7.23. cifs-utils

7.23.1. RHBA-2015:1366 — cifs-utils bug fix update

Updated cifs-utils packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The Server Message Block/Common Internet File System (SMB/CIFS) protocol is a standard file sharing protocol widely deployed on Microsoft Windows machines. The cifs-utils packages contain tools for mounting shares on Linux using the SMB/CIFS protocol. The tools in this package work in conjunction with support in the kernel to enable mounting a SMB/CIFS share onto a client and use it as if it were a standard Linux file system.

Bug Fix

BZ#1080482

Previously, attempts to mount a CIFS share failed when the system keytab was stored in a non-default location specified using the default_keytab_name setting in the /etc/krb5.conf file, even when the user provided the correct Kerberos credentials. However, mounting succeeded when default_keytab_name pointed to the default /etc/krb5.keytab file. The cifs.upcall helper process has been modified to respect non-default keytab locations provided using default_keytab_name. As a result, CIFS mount now works as expected even when the keytab is stored in a non-default location.

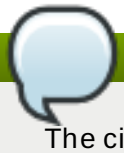
Users of cifs-utils are advised to upgrade to these updated packages, which fix this bug.

7.24. cim-schema

7.24.1. RHBA-2015:1267 — cim-schema bug fix and enhancement update

An updated cim-schema package that fixes several bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

The cim-schema package contains Common Information Model (CIM), a model for describing overall management information in a network or enterprise environment.



Upgrade to an upstream version

The cim-schema package has been upgraded to upstream version 2.33, which provides a number of model changes and enhancements over the previous version of the Final schema. This update also contains Experimental schema. (BZ#1087888)

Users of cim-schema are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

7.25. cluster

7.25.1. RHBA-2015:1363 — cluster bug fix and enhancement update

Updated cluster packages that fix several bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

The Red Hat Cluster Manager is a collection of technologies working together to provide data integrity and the ability to maintain application availability in the event of a failure.

Bug Fixes

BZ#1149516

Previously, the gfs2_convert utility or a certain corruption could introduce bogus values for the ondisk inode "di_goal_meta" field. Consequently, these bogus values could affect GFS2 block allocation, cause an EBADSLT error on such inodes, and could disallow the creation of new files in directories or new blocks in regular files. With this update, gfs2_convert calculates the correct values. The fsck.gfs2 utility now also has the capability to identify and fix incorrect inode goal values, and the described problems no longer occur.

BZ#1121693

The gfs2_quota, gfs2_tool, gfs2_grow, and gfs2_jadd utilities did not mount the gfs2 meta file system with the "context" mount option matching the "context" option used for mounting the parent gfs2 file system. Consequently, the affected gfs2 utilities failed with an error message "Device or resource busy" when run with SELinux enabled. The mentioned gfs2 utilities have been updated to pass the "context" mount option of the gfs2 file system to the meta file system, and they no longer fail when SELinux is enabled.

BZ#1133724

A race condition in the dlm_controld daemon could be triggered when reloading the configuration, which caused a dangling file pointer to be written to. Consequently, under certain rare conditions, dlm_controld could terminate unexpectedly with a segmentation fault, leaving Distributed Lock Manager (DLM) lockspaces unmanaged and requiring a system reboot to clear. This bug has been fixed, and dlm_controld no longer crashes when the configuration is updated.

BZ#1087286

Previously, errors generated while updating the resource-agents scheme were sometimes not reported. As a consequence, if an error occurred when updating the resource-agents schema, the update failed silently and later attempts to start the cman service could fail as well. With this update, schema errors are reported, and remedial action can be taken at upgrade time in case of problems.

Enhancements

BZ#1099223

The qdiskd daemon now automatically enables the master_wins mode when votes for the quorum disk default to 1 or when the number of votes is explicitly set to 1. As a result, quorum disk configuration is more consistent with the documentation, and a misconfiguration is avoided.

BZ#1095418

A new error message has been added to the qdiskd daemon, which prevents qdiskd from starting if it is configured with no heuristics in a cluster with three or more nodes. Heuristics are required in clusters with three or more nodes using a quorum device for correct operation in the event of a tie-break. Now, if no heuristics are specified and the cluster contains three or more nodes, the cman service fails to start and an error message is returned. This behavior prevents misconfigurations.

Users of cluster are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.26. clustermon

7.26.1. RHBA-2015:1413 — clustermon bug fix update

Updated clustermon packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The clustermon packages are used for remote cluster management. The modclusterd service provides an abstraction of cluster status used by the Conga architecture and by the Simple Network Management (SNMP) and Common Information Model (CIM) modules of clustermon.

Bug Fix

BZ#1111249, BZ#1114622

The internal ricci API has been extended with an ability to temporarily stop a clustered resource, which was used to resolve the BZ#1111249 enhancement request in the luci packages, documented in the RHBA-2015:20054 erratum.

Users of clustermon are advised to upgrade to these updated packages, which fix this bug.

7.27. coolkey

7.27.1. RHBA-2015:1370 — coolkey bug fix update

Updated coolkey packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The coolkey packages provide the coolkey smart card support library for the CoolKey, common access card (CAC), and personal identity verification (PIV) smart cards.

Bug Fix

BZ#1115626

Previously, after the user inserted a contactless PIV card, coolkey could not access it in a contactless way. As a consequence, the light indicating the card status started to blink inconsistently, and the Enterprise Security Client (ESC) failed to detect the card. With this patch, coolkey accesses the card certificate or key instead of the PIV authentication, PIV signing, or PIV key exchange keys. As a result, when the user inserts a contactless PIV card, ECS now successfully detects it.

Users of coolkey are advised to upgrade to these updated packages, which fix this bug.

7.28. corosync

7.28.1. RHBA-2015:1389 — corosync bug fix and enhancement update

Updated corosync packages that fix one bug and add two enhancements are now available for Red Hat Enterprise Linux 6.

The corosync packages provide the Corosync Cluster Engine and C Application Programming Interfaces (APIs) for Red Hat Enterprise Linux cluster software.

Bug Fix

BZ#1136431

When the corosync utility was configured with the IPv6 network and packet fragmentation was disabled on the Network Interface Controller (NIC) or switch, no packets were delivered. This update implements a correct calculation of the data fragment size, and packets are delivered as intended.

Enhancements

BZ#1163846

Earlier when using the UDP unicast (UDPU) protocol, all messages were sent to all the configured members, instead of being sent to only the active members. This makes sense for merge detection messages, otherwise it creates unnecessary traffic to missing members and can trigger excessive Address Resolution Protocol (ARP) requests on the network. The corosync code has been modified to only send messages to the missing members when it is required, otherwise to only send messages to the active ring members. Thus, most of the UDPU messages are now sent only to the active members with an exception of the messages required for proper detection of a merge or a new member (1-2 pkts/sec).

BZ#742999

With this update, the corosync packages have been modified to test whether the network interface has different IP address, port, and IP version when using the Redundant Ring Protocol (RRP) mode. Now, corosync properly checks correctness of the configuration file and prevents failures when using the RRP mode.

Users of corosync are advised to upgrade to these updated packages, which fix this bug and add these enhancements.

7.29. cpufrequtils

7.29.1. RHBA-2014:2015 — cpufrequtils bug fix update

Updated cpufrequtils packages that fix one bug and add one enhancement are now available for Red Hat Enterprise Linux 6.

The cpufrequtils packages contain utilities that can be used to control the cpufreq interface provided by the kernel on hardware that supports CPU frequency scaling.

Bug Fix

BZ#728999

Previously, the debug options in the package build scripts were disabled. Consequently, the debuginfo packages were not generated for the cpufrequtils utility. With this update, the debug options in the build scripts have been enabled, and debuginfo options are now available for cpufrequtils binary files.

Enhancement

BZ#730304

Prior to this update, the cpufreq-aperf utility was missing man pages. To provide the user with more information on cpufreq-aperf, the man pages have been added.

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

7.30. cpupowerutils

7.30.1. RHEA-2015:1437 — cpupowerutils enhancement update

Updated cpupowerutils packages that add one enhancement are now available for Red Hat Enterprise Linux 6.

The cpupowerutils packages provide a suite of tools to manage power states on appropriately enabled central processing units (CPU).

Enhancement

BZ#1187332

The turbostat utility now supports the 6th Generation Intel Core Processors – for mobile and desktop.

Users of cpupowerutils are advised to upgrade to these updated packages, which add this enhancement.

7.31. cpuspeed

7.31.1. RHBA-2015:1440 — cpuspeed bug fix update

Updated cpuspeed packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The cpuspeed packages contain a daemon that dynamically changes the speed of processors depending upon their current workload. These packages also allow users to enable CPU frequency scaling using in-kernel CPUfreq governors on Intel Centrino, AMD Athlon 64, and AMD Opteron platforms.

Bug Fix

BZ#1196755, BZ#1211828, BZ#1219780, BZ#1225024

A previous update brought in a change in the kernel introducing the intel_pstate driver, incompatible with how scaling was managed until Red Hat Enterprise Linux 6.7. Consequently, the cpuspeed service printed needless error messages during system boot and shutdown. With this update, platforms using intel_pstate support only the "performance" and "powersave" scaling governors, the default option and default state being "powersave". If the user has set a different governor from the above-mentioned, for example "ondemand" or "conservative", they have to edit the configuration and choose one from the two, "powersave" or "performance". In addition, needless error messages are no longer returned.

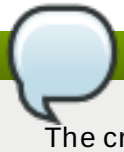
Users of cpuspeed are advised to upgrade to these updated packages, which fix this bug.

7.32. crash

7.32.1. RHBA-2015:1309 — crash bug fix and enhancement update

Updated crash packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The crash packages provide the core analysis suite, which is a self-contained tool that can be used to investigate live systems, as well as kernel core dumps created by the kexec-tools packages or the Red Hat Enterprise Linux kernel.



Upgrade to an upstream version

The crash packages have been upgraded to upstream version 7.1.0, which provides a number of bug fixes and enhancements over the previous version. (BZ#1111357)

Bug Fixes

BZ#1179480

A prior update of the AMD64 and Intel 64 kernels removed the STACKFAULT exception stack. As a consequence, using the "bt" command with the updated kernels previously displayed an incorrect exception stack name if the backtrace originated in an exception stack other than STACKFAULT. In addition, the "mach" command displayed incorrect names for exception stacks other than STACKFAULT. This update ensures that stack names are generated properly in the described circumstances, and both "bt" and "mach" now display correct information.

BZ#1208557

Attempting to run the crash utility with the vmcore and vmlinux files previously caused crash to enter an infinite loop and became unresponsive. With this update, the handling of errors when gathering tasks from pid_hash[] chains during session initialization has been

enhanced. Now, if a pid_hash[] chain has been corrupted, the patch prevents the initialization sequence from entering an infinite loop. This prevents the described failure of the crash utility from occurring. In addition, the error messages associated with corrupt or invalid pid_hash[] chains have been updated to report the pid_hash[] index number.

BZ#1073987

On certain system configurations, the "kmem -f", "kmem -F", and "kmem [address]" command options previously took a very long time to complete. This update increases the internal hash queue size used to store the address of each free page, and streamlines the free page search to only check the NUMA node that contains a specified address. As a result, the mentioned "kmem" options no longer have a negative impact on performance.

Enhancement

BZ#1195596

The makedumpfile command now supports the new sadump format that can represent more than 16 TB of physical memory space. This allows users of makedumpfile to read dump files over 16 TB, generated by sadump on certain upcoming server models.

Users of crash are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.33. cronie

7.33.1. RHBA-2015:0754 — cronie bug fix update

Updated cronie packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The cronie packages contain the standard UNIX daemon crond that runs specified programs at scheduled times and related tools. They are a fork of the original vixie-cron cron implementation and have security and configuration enhancements like the ability to use pam and SELinux.

Bug Fix

BZ#1204175

Due to a regression in parsing the /etc/anacrontab file caused by the previous cronie erratum released in the Fastrack channel, environment variables set in the /etc/anacrontab file were not recognized, and error messages were logged. These updated cronie packages fix the regression, and the variables are now set correctly for anacron jobs.

Users of cronie are advised to upgrade to these updated packages, which fix this bug.

7.33.2. RHBA-2015:0704 — cronie bug fix and enhancement update

Updated cronie packages that fix two bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

The cronie packages contain the standard UNIX daemon crond that runs specified programs at scheduled times and the anacron tool that enables crond to run jobs also on machines that are not continuously switched on.

Bug Fixes

BZ#1031383

Previously, the anacron process could terminate unexpectedly in cases when the anacrontab file contained incorrect configuration settings. To fix this bug, the configuration settings format check has been amended, and the anacron process no longer crashes.

BZ#1082232

Prior to this update, the crond pid file could be erroneously removed in case a crond sub-process terminated unexpectedly. With this update, handling of the crond sub-processes termination has been corrected, and the removal no longer occurs.

Enhancements

BZ#1108384

The crond daemon now logs shutdowns. Its proper terminations are therefore distinguishable from abnormal ones.

BZ#1123984

The crond daemon now logs errors when jobs are skipped due to getpwnam() call failures.

Users of cronie are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.34. cups

7.34.1. RHBA-2015:1346 — cups bug fix and enhancement update

Updated cups packages that fix several bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

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

Bug Fixes

BZ#951553

Incorrect reference for PageLogFormat in HTML documentation has been corrected, and PageLogFormat documentation is now accessible.

BZ#988062

Documentation for the operation of the CUPS Line Printer Daemon back-end "sanitize_title" option has been amended and now describes the option clearly.

BZ#1145064, BZ#1178370

Due to a problem with HTTP multipart handling in the CUPS scheduler, some browsers did not work as expected when attempting to add a printer using the web interface. A change from a later version has been backported enabling adding printers in all browsers without problems.

BZ#1161171

It was not possible to disable Secure Sockets Layer (SSLv3) and keep other secure

protocols enabled in CUPS. This left CUPS users vulnerable to the POODLE attack (CVE-2014-3566), and needing to deploy the stunnel utility for mitigation. This update disables SSLv3 support by default. For users who need to continue using SSLv3, an SSLOptions configuration directive has been added to the cupsd.conf file for the cupsd service and to the client.conf file for the client programs.

BZ#1164854

When the BrowsePoll configuration directive was used and the remote server configured for polling forbade access, the cups-polld process retried accessing immediately in a busy loop. The process consumed all processor time and increased network traffic. With this update, a mandatory delay of ten seconds has been introduced to prevent that. Affected users should also fix their configuration by removing the BrowsePoll line for the server, or adjusting the server to allow remote queries.

BZ#1170002

The CUPS scheduler incorrectly assumed the print queue still existed when there were only implicit classes with all members deleted due to being unresponsive. When sending a job using separate Create-Job and Send-Document requests to an implicit class whose members were being deleted, the CUPS scheduler terminated unexpectedly with a NULL dereference. The scheduler has been amended to respond with an error instead of crashing in this case.

BZ#1187840

A missing NULL check in job processing code caused the CUPS scheduler to terminate unexpectedly when a job with more than one file aborted due to a filter failure. This update adds the check to prevent the CUPS scheduler from crashing in the described situation.

BZ#1196217

The ErrorPolicy configuration directive was not validated on startup, and an unintended default error policy could be used without a warning. The directive is now validated on startup and reset to the default if the configured value is incorrect. The intended policy is used, or a warning message is logged.

BZ#1198394

Due to an incomplete fix in a prior update, some environment variables were not correctly set on startup, which led to SELinux denials. The remainder of the original fix has been added, and the variables are now set correctly on startup.

Enhancements

BZ#1115219

It is now possible to direct jobs to a single printer with failover to other printers instead of using load balancing among printers that is built into CUPS. Jobs can be directed to the first working printer of a set, the preferred printer, with other printers used only if the preferred one is unavailable.

BZ#1120587

Description of the ErrorPolicy directive with supported values has been added to the cupsd.conf(5) man page. The ErrorPolicy directive defines the default policy used when a back end is unable to send a print job to the printer.

Users of CUPS are advised to upgrade to these updated packages, which fix these bugs and add these enhancements. After installing this update, the cupsd service will be restarted automatically.

7.35. curl

7.35.1. RHSA-2015:1254 — Moderate: curl security, bug fix, and enhancement update

Updated curl packages that fix multiple security issues, several bugs, and add two enhancements are now available for Red Hat Enterprise Linux 6.

Red Hat Product Security 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 curl packages provide the libcurl library and the curl utility for downloading files from servers using various protocols, including HTTP, FTP, and LDAP.

Security Fixes

CVE-2014-3613

It was found that the libcurl library did not correctly handle partial literal IP addresses when parsing received HTTP cookies. An attacker able to trick a user into connecting to a malicious server could use this flaw to set the user's cookie to a crafted domain, making other cookie-related issues easier to exploit.

CVE-2014-3707

A flaw was found in the way the libcurl library performed the duplication of connection handles. If an application set the CURLOPT_COPYPOSTFIELDS option for a handle, using the handle's duplicate could cause the application to crash or disclose a portion of its memory.

CVE-2014-8150

It was discovered that the libcurl library failed to properly handle URLs with embedded end-of-line characters. An attacker able to make an application using libcurl to access a specially crafted URL via an HTTP proxy could use this flaw to inject additional headers to the request or construct additional requests.

CVE-2015-3143, **CVE-2015-3148**

It was discovered that libcurl implemented aspects of the NTLM and Negotatiate authentication incorrectly. If an application uses libcurl and the affected mechanisms in a specifc way, certain requests to a previously NTLM-authenticated server could appears as sent by the wrong authenticated user. Additionally, the initial set of credentials for HTTP Negotiate-authenticated requests could be reused in subsequent requests, although a different set of credentials was specified.

Red Hat would like to thank the cURL project for reporting these issues.

Bug Fixes

BZ#1154059

An out-of-protocol fallback to SSL version 3.0 (SSLv3.0) was available with libcurl. Attackers could abuse the fallback to force downgrade of the SSL version. The fallback has

been removed from libcurl. Users requiring this functionality can explicitly enable SSLv3.0 through the libcurl API.

BZ#883002

A single upload transfer through the FILE protocol opened the destination file twice. If the inotify kernel subsystem monitored the file, two events were produced unnecessarily. The file is now opened only once per upload.

BZ#1008178

Utilities using libcurl for SCP/SFTP transfers could terminate unexpectedly when the system was running in FIPS mode.

BZ#1009455

Using the "--retry" option with the curl utility could cause curl to terminate unexpectedly with a segmentation fault. Now, adding "--retry" no longer causes curl to crash.

BZ#1120196

The "curl --trace-time" command did not use the correct local time when printing timestamps. Now, "curl --trace-time" works as expected.

BZ#1146528

The valgrind utility could report dynamically allocated memory leaks on curl exit. Now, curl performs a global shutdown of the NetScape Portable Runtime (NSPR) library on exit, and valgrind no longer reports the memory leaks.

BZ#1161163

Previously, libcurl returned an incorrect value of the CURLINFO_HEADER_SIZE field when a proxy server appended its own headers to the HTTP response. Now, the returned value is valid.

Red Hat would like to thank the cURL project for reporting these issues.

Enhancements

BZ#1012136

The "--tlsv1.0", "--tlsv1.1", and "--tlsv1.2" options are available for specifying the minor version of the TLS protocol to be negotiated by NSS. The "--tlsv1" option now negotiates the highest version of the TLS protocol supported by both the client and the server.

BZ#1058767, BZ#1156422

It is now possible to explicitly enable or disable the ECC and the new AES cipher suites to be used for TLS.

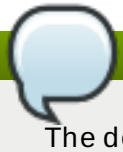
All curl users are advised to upgrade to these updated packages, which contain backported patches to correct these issues and add these enhancements.

7.36. dejavu-fonts

7.36.1. RHBA-2015:1327 — dejavu-fonts bug fix and enhancement update

Updated dejavu-fonts packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The DejaVu fonts are a font family based on the Vera Fonts. Its purpose is to provide a wider range of characters while maintaining the original look and feel through the process of collaborative development.



Upgrade to an upstream version

The dejavu-fonts packages have been upgraded to upstream version 2.33, which provides a number of bug fixes and enhancements over the previous version. Notably, this adds a number of new characters and symbols to the supported fonts. (BZ#1060882)

Users of dejavu-fonts are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.37. device-mapper-multipath

7.37.1. RHBA-2015:1391 — 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 6.

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

Bug Fixes

BZ#880121

If the multipathd daemon failed to add a multipath device, in some circumstances, it was freeing the alias and then accessing it and attempting to free it again. Consequently, multipathd terminated unexpectedly. With this update, multipathd no longer frees the alias twice, or attempts to access the freed alias, and thus no longer crashes in the described situation.

BZ#1120047

Previously, any target port with the ALUA preference bit set was given a higher priority than all other target ports. Consequently, when a target port had the preference bit set, multipath did not balance load between it and other ports that were equally optimized. With this update, the preference bit only increases the priority of paths that are not already optimized. Now, if the preference bit is set on a non-optimized port, the port is used. However, if the preference bit is set on an optimized port, all optimized ports are used, and multipath loads balance across them.

BZ#1136966

When the parted utility created partitions on an existing multipath device, it raced with the kpartx utility to create the partitions. This could cause device or resource busy errors. Now, kpartx only creates partition devices when the multipath device is activated, and no longer automatically creates partitions when parted is run on existing multipath devices.

BZ#1148096

Previously, a multipath device was not assigned a user_friendly_name by initramfs, which caused a conflict with the name already assigned by the normal system. Because of the name conflict, multipath could try to update the wrong device, and thus cause data corruption. To fix this bug, multipath checks paths to see if a device's user_friendly_name is already assigned, and assigns a new one if it is.

BZ#1171862

Previously, the libmultipath utility was keeping a global cache of sysfs data for all programs, even though this was only necessary for the multipathd daemon. As a consequence, a memory error could occur when multiple threads were using libmultipath without locking. This led to unexpected termination of multithreaded programs using the mpath_persistent_reserve_in() or mpath_persistent_reserve_out() functions. With this update, only multipathd uses the global sysfs data cache, and the described crashes are thus avoided.

BZ#1175888

Previously, the first time the multipath utility recognized a path device, the path device was not claimed in the udev utility, and other programs could race multipath to claim it. As a consequence, multipath systems could fail to boot during installation. With this update, the multipathd daemon now checks the kernel command line on startup. If it has recognized any parameters with a World Wide Identifier (WWID) value, it adds those WWIDs to the list of multipath WWIDs. Devices with those WWIDs are thus claimed the first time they are recognized. As a result, if multipath systems do not boot successfully during installation, users can add mpath.wwid=[WWID] to the kernel command line to work around the problem.

Enhancements

BZ#978947

This update adds new built-in configuration for Dell MD36xxf storage arrays.

BZ#997028

With this udpate, multipath autodetects whether an EMC CLARiiON array is set up in ALUA or PNR mode, and correctly configures itself to match.

BZ#1072081

Now, the multipathd daemon has two new configuration options "delay_watch_checks" and "delay_wait_checks". The user is recommended to refer to the multipath(8) man page for more information.

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

7.38. dhcp

7.38.1. RHBA-2015:1258 — dhcp bug fix and enhancement update

Updated dhcp packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The Dynamic Host Configuration Protocol (DHCP) is a protocol that allows individual devices on an IP network to get their own network configuration information, including an IP address, a subnet

mask, and a broadcast address. The dhcp packages provide a relay agent and ISC DHCP service required to enable and administer DHCP on a network.

Bug Fixes

BZ#1130804

Previously, the DHCPv6 client was sometimes started to configure a network interface which was not fully loaded. Consequently, dhclient failed to run because the network interface did not have a link-local address yet, which the DHCPv6 client requires. This update adds a wait loop into dhclient-script, and dhclient no longer fails due to a missing link-local address.

BZ#1150587

When the dhcpd daemon was using a plain interface as well as an interface configured as a VLAN trunk, and the dhcpd daemon was configured to listen only on the plain interface, it detected traffic also from VLAN networks, regardless of the configuration. As a consequence, dhcpd was generating incorrect responses. With this update, the bug has been corrected, and in the described scenario, dhcpd now ignores tagged requests, and thus generates correct responses.

BZ#1151054

When running the DHCPv6 relay agent and the "lower" interface was specified ("-l") on the command line before the "upper" interface ("-u"), message relaying did not work. The underlying source code has been fixed, and DHCPv6 relay agent now relays messages properly.

BZ#1185075

When a large number of nodes with InfiniBand network cards booted at the same time, some nodes were assigned duplicate IP addresses. With this update, generation of the xid field in DHCP messages sent by the client has been fixed for the xid fields to be unique, and nodes are now assigned unique IP addresses as expected.

BZ#1187967

Previously, attempting to run the dhcrelay and dhcrelay6 services simultaneously prevented the latter service from starting. The dhcrelay6 init script has been fixed, and running both dhcrelay and dhcrelay6 services no longer causes problems.

Enhancement

BZ#1058674

With this update, the dhcpd daemon is able to handle dhcp option 97 - Client Machine Identifier (pxe-client-id), so it is now possible to statically allocate an IP address for a particular client based on its identifier, sent in option 97.

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

7.39. dmidecode

7.39.1. RHBA-2015:1425 — dmidecode bug fix update

Updated dmidecode packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The dmidecode packages provide 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.

Bug Fix

BZ#1192357

Prior to this update, the dmidecode utility did not support the DDR4 type of memory. Consequently, compiling of the dmidecode code for hardware with DDR4 memory type gave out of specs results. With this update, dmidecode has been updated so that the DDR4 is among memory types and no longer returns out of specs while compiling the dmidecode source code.

Users of dmidecode are advised to upgrade to these updated packages, which fix this bug.

7.40. dovecot

7.40.1. RHBA-2015:1348 — dovecot bug fix and enhancement update

Updated dovecot packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

Dovecot is an IMAP server for Linux and other UNIX-like systems, primarily written with security in mind. It also contains a small POP3 server, and supports e-mail in either the maildir or mbox format. The SQL drivers and authentication plug-ins are provided as subpackages.

Bug Fixes

BZ#723228

The ports used by dovecot were in some cases unavailable during the boot process by other services, which caused dovecot to fail to start and display an "Address already in use" error. This update configures the portreserve service to ensure that dovecot's ports stay available during the boot process, which prevents the described failure from occurring.

BZ#771336

Previously, the dovecot utility used too small a login input buffer for Kerberos authentication. As a consequence, users who attempted to use Kerberos authentication were not able to log in. This updated version of dovecot uses a bigger input buffer, and users can now authenticate to their email accounts using a Kerberos ticket.

BZ#813957

Prior to this update, dovecot logged a redundant "unable to get certificate" error message when no certification revocation list (CRL) was available. With this update, dovecot no longer treats missing CRL as an error, and no longer logs an error in the mentioned scenario.

BZ#961466

When the LIST-STATUS extension was used with certain hierarchy separator symbols, dovecot in some cases terminated unexpectedly. Consequently, the user was unable to list the contents of their e-mail folder. This update fixes the code for traversing folders, and using LIST-STATUS no longer causes dovecot to crash.

BZ#1131749

Previously, after executing the "uid copy" command against a non-existent mailbox, the dovecot server became unresponsive. As a consequence, the user could not download e-mails unless recovered manually. A patch has been provided to fix this bug, and dovecot no longer hangs in the aforementioned scenario.

Enhancement

BZ#1153041

With this update, it is possible to configure which Secure Sockets Layer (SSL) protocols dovecot allows. Among other things, this allows users to disable SSLv3 connections and thus mitigate the impact of the POODLE vulnerability. Due to security concerns, SSLv2 and SSLv3 are now also disabled by default, and the user has to be allow them manually if required.

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

7.41. dracut

7.41.1. RHBA-2015:1328 — dracut bug fix and enhancement update

Updated dracut packages that fix several bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

The dracut packages include an event-driven initramfs generator infrastructure based on the udev device manager. The virtual file system, initramfs, is loaded together with the kernel at boot time and initializes the system, so it can read and boot from the root partition.

Bug Fixes

BZ#1198117

Previously, the dracut utility incorrectly printed an error message if the /tmp/net.$netif.override file did not exist. With this update, dracut verifies whether /tmp/net.$netif.override exists before it attempts to read it, which prevents the described error from occurring.

BZ#1005886

Prior to this update, the dracut logrotate configuration determined that the "time" option had priority over the "size" option. Consequently, the dracut logs were rotated only yearly regardless of their size. This update removes the "time" option of the logrotate configuration, and the dracut logs now rotate when the size exceeds 1 MB.

BZ#1069275

If "ip=ibft" was specified as a kernel command-line argument, but the "ifname=<iface>:<mac>" parameter was not, dracut did not handle network interfaces correctly. As a consequence, iSCSI disks were not connected to the system, and thus the system failed to

boot. With this update, dracut handles "ip=ibft" as a kernel command-line argument, even without "ifname=<iface>:<mac>", and iSCSI disks are now connected to the system successfully resulting in successful system boot.

BZ#1085562

If the /etc/crypttab file did not contain a new line as the last character, dracut failed to parse the last line of the file, and the encrypted disk could not be unlocked. This update fixes dracut to handle /etc/crypttab without a new line at the end, and the encrypted disk specified on the last line is now handled as expected, requesting a password and unlocking the disk.

BZ#1130565

If the /etc/lvm/lvm.conf file had host tags defined, the initramfs virtual file system did not insert the /etc/lvm/lvm_hostname.conf file during kernel upgrade, which previously led to a boot failure. This update adds /etc/lvm/lvm_hostname.conf along with /etc/lvm/lvm.conf, and the system now boots with host tags as intended.

BZ#1176671

Previously, dracut did not parse the kernel command line correctly for some iSCSI parameters, which led to iSCSI disks not being connected. With this update, dracut parses the kernel command-line parameters for iSCSI correctly, and iSCSI disks are now connected successfully.

BZ#1184142

Due to an internal change in the nss-softokn-freebl package, dracut could not build an initramfs file in FIPS mode. To fix this bug, nss-softokn-freebl delivers its own dracut module and dracut now requires nss-softokn-freebl as a dependency. As a result, dracut can build FIPS-enabled initramfs with all files.

BZ#1191721

When network parameters were specified on the kernel command line, dracut only attempted to connect to iSCSI targets provided the network could be brought up. Consequently, for misconfigured networks, iSCSI firmware settings or iSCSI offload connections were not explored. To fix this bug, dracut now attempts to connect to the iSCSI targets even if after a certain timeout no network connection can be brought up. As a result, iSCSI targets can be connected even for misconfigured kernel command-line network parameters.

BZ#1193528

Due to changes in FIPS requirements, a new deterministic random-byte generator (drbg) was added to the kernel for FIPS purposes. With this update, dracut loads drbg as other kernel modules in FIPS mode.

Enhancements

BZ#1111358

With this update, dracut can boot from iSCSI on a network with VLANs configured, where the VLAN settings are stored in the iBFT BIOS.

BZ#1226905

LVM thin volumes are now supported in initramfs.

Users of dracut are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.42. dstat

7.42.1. RHEA-2015:1290 — dstat enhancement update

An updated dstat package that adds one enhancement is now available for Red Hat Enterprise Linux 6.

The dstat package provides a replacement for the vmstat, iostat, and netstat tools. The dstat tool can be used for performance tuning tests, benchmarks, and troubleshooting.

Enhancement

BZ#766443

The dstat utility has been enhanced to support the use of symbolic links as its parameters. This allows users to dynamically specify the boot device name, which ensures that dstat displays correct information after hot plugs and similar operations.

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

7.43. e2fsprogs

7.43.1. RHBA-2015:1442 — e2fsprogs bug fix update

Updated e2fsprogs packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The e2fsprogs packages provide a number of utilities for creating, checking, modifying, and correcting any inconsistencies in the ext2 file systems.

Bug Fix

BZ#1218262

Previously, if the superblock of an ext2, ext3, or ext4 file system contained a "last mount" or "last check" time which was set in the future, the e2fsck utility did not fix the error in "preen" mode. As a consequence, an incorrect system clock could stop the boot process and wait for an administrator intervention due to a failed boot-time file system check. With this update, these time-stamp errors are fixed automatically in "preen" mode, and the boot process is no longer interrupted in the described situation.

Users of e2fsprogs are advised to upgrade to these updated packages, which fix this bug.

7.44. edac-utils

7.44.1. RHBA-2015:1430 — edac-utils bug fix update

Updated edac-utils packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The edac-utils packages contain Error Detection And Correction (EDAC), the current set of drivers in the Linux kernel that handles detection of ECC errors from memory controllers for most chipsets on the 32-bit and 64-bit architectures. The user-space component consists of an init script which

ensures that EDAC drivers and Dual Inline Memory Module (DIMM) labels are loaded at system startup, as well as a library and utility for reporting current error counts from the EDAC sysfs files.

Bug Fix

BZ#1200884

Previously, the libsysfs packages were not listed as a dependency for the edac-utils packages. As a consequence, on systems where the libsysfs packages were not installed independently, the edac-utils packages were not fully functional due to the lack of libraries provided by libsysfs. This update adds libsysfs to the list of dependencies for edac-utils. As a result, libsysfs can be automatically installed together with edac-utils, thus providing all the libsysfs libraries necessary for edac-utils to work properly on all systems.

Users of edac-utils are advised to upgrade to these updated packages, which fix this bug.

7.45. efibootmgr

7.45.1. RHBA-2015:1431 — efibootmgr bug fix update

Updated efibootmgr packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The efibootmgr utility is responsible for the boot loader installation on Unified Extensible Firmware Interface (UEFI) systems.

Bug Fix

BZ#1151681

Previously, when the installation of the Generation 2 Virtual Machine (Gen2 VM) on the Hyper-V 2012 and R2 host was completed, the VM disappeared from the Virtual Machines list. As a consequence, the Hyper-V Manager could no longer load the VM settings, which rendered the VM unusable. With this update, the bug in the efibootmgr packages has been fixed so that the VM settings are accessible in the described scenario.

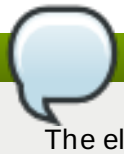
Users of efibootmgr are advised to upgrade to these updated packages, which fix this bug.

7.46. elfutils

7.46.1. RHEA-2015:1302 — elfutils bug fix and enhancement update

Updated elfutils packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The elfutils packages contain a number of utility programs and libraries related to the creation and maintenance of executable code.



Upgrade to an upstream version

The elfutils packages have been upgraded to upstream version 0.161, which provides a number of bug fixes and enhancements over the previous version. (BZ#1167724)

Bug Fix

BZ#1167724

The eu-stack utility supports showing inlined frames and it is now able to produce backtraces even for processes that might have some of their on-disk libraries updated or deleted.

- Improved DWZ compressed DWARF multi-file support with new functions, "dwarf_getalt" and "dwarf_setalt", has been introduced.
- Support for ARM 64-bit architecture and Red Hat Enterprise Linux for POWER, little endian has been added.
- The libdw library now supports LZMA-compressed (.ko.xz) kernel modules.
- Support for ".debug_macro" has been added; new functions has been introduced: "dwarf_getmacros_off", "dwarf_macro_getsrcfiles", "dwarf_macro_getparamcnt", and "dwarf_macro_param".
- New GNU extensions to the DWARF format are now recognized.
- New functions have been added to the libdw library: "dwarf_peel_type", "dwarf_cu_getdwarf", "dwarf_cu_die", "dwelf_elf_gnu_debuglink", "dwelf_dwarf_gnu_debugaltlink", "dwelf_elf_gnu_build_id".

Users of elfutils are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.47. emacs

7.47.1. RHBA-2015:0238 — emacs bug fix update

Updated emacs packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

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.

Bug Fixes

BZ#852516

Previously, the data_space_start value was set inaccurately. As a consequence, the emacs text editor returned the following memory warning message:

Emergency (alloc): Warning: past 95% of memory limit

To fix this bug, data_space_start has been set correctly, and emacs no longer returns warning messages.

BZ#986989

When using the glyph face encoding, a text face was not removed from the garbage collector. As a consequence, the emacs text editor terminated unexpectedly with a segmentation fault when attempting to remove the face. With this update, the text face is also removed from the garbage collector, and emacs thus no longer crashes in the described scenario.

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

7.48. enchant

7.48.1. RHBA-2015:0668 — enchant bug fix update

Updated enchant packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The enchant packages contain a library that wraps other spell-checking back ends.

Bug Fix

BZ#1015310

Previously, the enchant library opened the user's custom dictionary file in write mode. Consequently, the content of the file was always erased, and any words added to the dictionary earlier were forgotten. With this update, the dictionary file is opened in append mode. As a result, new additions to the custom dictionary no longer delete previously saved words.

Users of enchant are advised to upgrade to these updated packages, which fix this bug.

7.49. environment-modules

7.49.1. RHBA-2015:0670 — environment-modules bug fix update

Updated environment-modules packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The environment-modules packages provide for the dynamic modification of user environment using module files. Each module file contains the information needed to configure the shell for an application. Once the package is initialized, the environment can be modified on a per-module basis using the module command which interprets module files.

Bug Fixes

BZ#979789

Previously, misleading information about available modules in nested module directories was displayed to the user. To fix this bug, the code detecting module versions has been amended, and correct information is now displayed.

BZ#1117307

Prior to this update, modules were not properly unloaded when a loading module file contained the "module unload" command. With this update, the logic in the code for version detection of modules has been modified, and modules that contain the "module unload" command are now unloaded correctly.

Users of environment-modules are advised to upgrade to these updated packages, which fix these bugs.

7.50. ethtool

7.50.1. RHEA-2015:1306 — ethtool enhancement update

Updated ethtool packages that add one enhancement are now available for Red Hat Enterprise Linux 6.

The ethtool packages provide the ethtool utility that enables querying and changing settings such as speed, port, autonegotiation, PCI locations, and checksum offload on many network devices, especially of Ethernet devices.

Enhancement

BZ#1066605

This update enables the ethtool utility to accept a user-defined Receive-Side Scaling (RSS) hash key value for the Ethernet driver, which improves the performance and security of RSS. As a result, the user can set the RSS hash key value for the Ethernet driver with ethtool.

Users of ethtool are advised to upgrade to these updated packages, which add this enhancement.

7.51. evolution-data-server

7.51.1. RHBA-2015:1264 — evolution-data-server bug fix update

Updated evolution-data-server packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The evolution-data-server packages provide a unified back end for applications which interact with contacts, tasks and calendar information. Evolution Data Server was originally developed as a back end for the Evolution information management application, but is now used by various other applications.

Bug Fixes

BZ#1163375

The Evolution client could not connect to a mail server using the Secure Sockets Layer (SSL) protocol when the server had SSL disabled due to the POODLE vulnerability. With this update, the Evolution Data Server has been modified to also connect using the Transport Layer Security (TLSv1) protocol, thus fixing this bug.

BZ#1141760

Previously, the e-calendar-factory process did not terminate automatically when the user logged out of the graphical desktop environment, and e-calendar-factory thus redundantly consumed system resources. This update fixes the underlying code, which prevents this problem from occurring.

Users of evolution-data-server are advised to upgrade to these updated packages, which fix these bugs.

7.52. evolution-exchange

7.52.1. RHBA-2015:1265 — evolution-exchange bug fix update

Updated evolution-exchange packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The evolution-exchange packages enable added functionality to Evolution when used with a Microsoft Exchange Server 2003. The packages also contain Exchange Web Services (EWS) connector, which can connect to Microsoft Exchange 2007 and later servers.

Bug Fix

BZ#1160279

When the Exchange Web Services (EWS) connector was used, the UI part of the connector failed to load due to a missing external symbol. Consequently, the user could neither change the settings nor configure a new mail account for the EWS part of the evolution-exchange packages. This update corrects the library link options during build time to have the missing symbol available. Now, the UI part of the EWS connector loads properly, and the mail account can be added and configured.

Users of evolution-exchange are advised to upgrade to these updated packages, which fix this bug.

7.53. fence-agents

7.53.1. RHBA-2015:1350 — fence-agents bug fix and enhancement update

Updated fence-agents packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The fence-agents packages provide a collection of scripts for handling remote power management for cluster devices. They allow failed or unreachable nodes to be forcibly restarted and removed from the cluster.

Upgrade to an upstream version

The fence-agents packages have been upgraded to upstream version 4.0.15, which provides a number of bug fixes and enhancements over the previous version.

Bug Fix

BZ#1049805, BZ#1094515, BZ#1099551, BZ#1111482, BZ#1118008, BZ#1123897, BZ#1171734

This update adds the "--tls1.0" option to the fence agent for HP Integrated Lights-Out 2 (iLO2) devices. With this option, iLO2 negotiation of the TLS protocol works as expected when using an iLO2 device with firmware version 2.27.

- The fence_kdump agent now supports the "monitor" action, making integration with a cluster stack easier.
- The fence-agents packages now support the fence_ilo_moonshot fence agent for HP Moonshot iLO devices. For information on the fence_ilo_moonshot parameters, see the fence_ilo_moonshot(8) man page.
- This update adds support for the fence_ilo_ssh fence agent. The agent logs into an iLO device using SSH and reboots a specified outlet. For information on the fence_ilo_ssh parameters, see the fence_ilo_ssh(8) man page.

- This update adds support for the fence_mpath fence agent. This agent is an I/O fencing agent that uses SCSI-3 persistent reservations to control access to multipath devices. For information on fence_mpath and its parameters, see the fence_mpath(8) man page.
- The fence agent for APC devices over Simple Network Management Protocol (SNMP) has been updated to support the latest versions of the APC firmware.
- This update adds support for the fence_emerson fencing agent for Emerson devices over Simple Network Management Protocol (SNMP). It is an I/O fencing agent that can be used with the MPX and MPH2 Emerson devices. For information on the parameters for the fence_emerson fencing agent, see the fence_emerson(8) man page.

Users of fence-agents are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.54. fence-virt

7.54.1. RHBA-2015:1401 — fence-virt bug fix and enhancement update

Updated fence-virt packages that fix two bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The fence-virt packages provide a fencing agent for virtual machines, as well as a host agent that processes fencing requests.

Bug Fixes

BZ#1125290

Previously, the fence-virt utility in some case incorrectly returned a zero exit code when it detected an error in processing a request. With this update, the static analysis errors that caused this problem have been fixed, and fence-virt now returns appropriate error codes if it detects an error.

BZ#1078197

Due to an incorrectly configured range of supported TCP and multicast ports, fence-virt did previously not work properly with certain ports. This update fixes the range of supported TCP and multicast ports, which prevents the problem form occurring.

Enhancement

BZ#1020992

When the fence-virt and fence-xvm utilities are invoked with the "-o status" parameter, they now print their status in a more comprehensible manner, as either "Status: ON" or "Status: OFF".

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

7.55. fprintd

7.55.1. RHBA-2015:0663 — fprintd bug fix update

Updated fprintd packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The fprintd packages contain a D-Bus service to access fingerprint readers.

Bug Fix

BZ#1024825

Due to a bug in the fprintd daemon code, long-running Pluggable Authentication Module (PAM) clients were experiencing file descriptor leaks for each iteration of authentication. With this update, the file descriptor closes after completing its job, and therefore the file descriptor leaks no longer occur.

Users of fprintd are advised to upgrade to these updated packages, which fix this bug.

7.56. freeradius

7.56.1. RHSA-2015:1287 — Moderate: freeradius security, bug fix, and enhancement update

Updated freeradius packages that fix one security issue, several bugs, and add various enhancements are now available for Red Hat Enterprise Linux 6.

Red Hat Product Security 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.

FreeRADIUS is a high-performance and highly configurable free Remote Authentication Dial In User Service (RADIUS) server, designed to allow centralized authentication and authorization for a network.

Security Fix

CVE-2014-2015

A stack-based buffer overflow was found in the way the FreeRADIUS rlm_pap module handled long password hashes. An attacker able to make radiusd process a malformed password hash could cause the daemon to crash.

Note

The freeradius packages have been upgraded to upstream version 2.2.6, which provides a number of bug fixes and enhancements over the previous version. (BZ#1078736)

Bug Fixes

BZ#1078736

The number of dictionaries have been updated.

* This update implements several Extensible Authentication Protocol (EAP) improvements.

* A number of new expansions have been added, including: %{randstr:...}, %{hex:...}, %{sha1:...}, %{base64:...}, %{tobase64:...}, and %{base64tohex:...}.

* Hexadecimal numbers (0x...) are now supported in %{expr:...} expansions.

* This update adds operator support to the rlm_python module.

* The Dynamic Host Configuration Protocol (DHCP) and DHCP relay code have been finalized.

* This update adds the rlm_cache module to cache arbitrary attributes.

For a complete list of bug fixes and enhancements provided by this rebase, see the freeradius changelog linked to in the References section.

BZ#904578

The /var/log/radius/radutmp file was configured to rotate at one-month intervals, even though this was unnecessary. This update removes /var/log/radius/radutmp from the installed logrotate utility configuration in the /etc/logrotate.d/radiusd file, and /var/log/radius/radutmp is no longer rotated.

BZ#921563

The radiusd service could not write the output file created by the raddebug utility. The raddebug utility now sets appropriate ownership to the output file, allowing radiusd to write the output.

BZ#921567

After starting raddebug using the "raddebug -t 0" command, raddebug exited immediately. A typo in the special case comparison has been fixed, and raddebug now runs for 11.5 days in this situation.

BZ#1060319

MS-CHAP authentication failed when the User-Name and MS-CHAP-User-Name attributes used different encodings, even when the user provided correct credentials. Now, MS-CHAP authentication properly handles mismatching character encodings. Authentication with correct credentials no longer fails in this situation.

BZ#1135439

Automatically generated default certificates used the SHA-1 algorithm message digest, which is considered insecure. The default certificates now use the more secure SHA-256 algorithm message digest.

BZ#1142669

During the Online Certificate Status Protocol (OCSP) validation, radiusd terminated unexpectedly with a segmentation fault after attempting to access the next update field that was not provided by the OCSP responder. Now, radiusd does not crash in this situation and instead continues to complete the OCSP validation.

BZ#1173388

Prior to this update, radiusd failed to work with some of the more recent MikroTIK attributes, because the installed directory.mikrotik file did not include them. This update adds MikroTIK attributes with IDs up to 22 to dictionary.mikrotik, and radiusd now works as expected with these attributes.

Users of freeradius are advised to upgrade to these updated packages, which correct these issues and add these enhancements. After installing this update, the radiusd service will be restarted automatically.

7.57. gcc

7.57.1. RHBA-2015:1339 — gcc bug fix and enhancement update

Updated gcc packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

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

Bug Fixes

BZ#1190640

Previously, due to a bug in the stdarg functions optimization, the compiler could produce incorrect code. The problem occurred only when the va_list variable escaped a PHI node. This bug has been fixed, and the compiler now generates correct code.

BZ#1150606

Previously, when the vectorization optimization was enabled, the compiler could extract a scalar component of a vector with element types whose precision did not match the precision of their mode. Consequently, GCC could terminate unexpectedly while trying to vectorize a code that was using bit-fields. With this update, the compiler no longer vectorizes such code, and the code now compiles correctly.

BZ#1177458

Previously, the compiler did not properly handle incorrect usage of the PCH (Precompiled Headers) feature. When a PCH file was not included as the first include, the compiler terminated unexpectedly with a segmentation fault. The compiler has been fixed not to use such incorrect includes, and it no longer crashes in this scenario.

BZ#1134560

In previous versions of the GNU Fortran compiler, the type specifiers for Cray pointees were incorrectly overwritten by the type specifiers of components with the same name. Consequently, compiling failed with an error message. This bug has been fixed, and the Cray pointers are now handled correctly.

Enhancement

BZ#1148120

The gcc hotpatch attribute implements support for online patching of multithreaded code on System z binaries. With this update, it is possible to select specific functions for hotpatching using a "function attribute" and to enable hotpatching for all functions using the "-mhotpatch=" command-line option. As enabled hotpatching has negative impact on software size and performance, it is recommended to use hotpatching for specific functions and not to enable hotpatch support in general.

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

7.58. gcc-libraries

7.58.1. RHBA-2015:1429 — gcc-libraries bug fix and enhancement update

Updated gcc-libraries packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The gcc-libraries packages contain various GNU Compiler Collection (GCC) runtime libraries, such as libatomic and libitm.

Upgrade to an upstream version

The gcc-libraries packages have been upgraded to upstream version 5.0.0, which provides a number of bug fixes and enhancements over the previous version. These enhancements are required by the features that will be present in future releases of Red Hat Developer Toolset.

Among other changes, a new package "libmpx" is now available, which contains Memory Protection Extensions runtime libraries. (BZ#1201767)

Users of gcc-libraries are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.59. gdb

7.59.1. RHBA-2015:1325 — gdb bug fix update

Updated gdb packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The GNU Debugger (GDB) allows users to debug programs written in various programming languages including C, C++, and Fortran.

Bug Fixes

BZ#1099929

When GDB found a thread with PID -1, GDB attempted to attach to that incorrect PID and consequently failed with an internal error. With this update, GDB detects the incorrect PID -1 earlier and displays a warning message to the user. In addition, the debugging session is no longer affected by the scenario described above.

BZ#1117841

GDB used a splay tree to store elements related to address maps. However, when iterating through splay trees that were too large, the recursion of the splay_tree_foreach_helper() function caused GDB to run out of stack, which generated a segmentation fault. The implementation of splay_tree_foreach_helper() has been changed to non-recursive, which improves the efficiency of iterator() and makes GDB avoid the aforementioned failure.

BZ#1119119

Previously, GDB did not check for a NULL pointer when trying to find the charset names from the user environment. This caused GDB to terminate unexpectedly, generating a segmentation fault. With this update, GDB correctly checks if it is dealing with a NULL file pointer, thus fixing the bug.

BZ#1139405

GDB uses the "(anonymous namespace)" string in the string representation of any symbol defined in an anonymous namespace. However, the linespec parser did not recognize that this string was a necessary component, symbol lookups failed and breakpoints could not set or reset on symbols defined in anonymous namespaces. To fix this bug, the anonymous namespace recognition has been abstracted to clarify the unique role of this representation requirement. Additionally, the linespec parser has been updated to properly deal with the required string. As a result, breakpoints on symbols in anonymous namespaces can be properly set or reset by GDB.

BZ#1149205

The "catch syscall" command uses a special type of breakpoint inside GDB, which is not maintained by the code that handles normal breakpoints. Previously, GDB was not able to properly catch a system call in the parent process after the fork() function call. With this update, system call catchpoints are no longer removed from a program that forked itself, and GDB is now able to correctly stop at a call from the parent process after it has forked.

BZ#1156192

A defect in the dlopen() library function previously caused recursive calls to dlopen() to crash or abort with a library assertion. Recursive calls to dlopen() may occur if an implementation of malloc() provided by the user calls dlopen(). The dlopen implementation is now reentrant, and recursive calls to dlopen() no longer crash or abort with an assertion.

BZ#1162264

Under certain conditions, while attaching to a process, GDB can perform the initial low level ptrace attach request, but the kernel previously refused to let the debugger finish the attach sequence. Consequently, GDB terminated unexpectedly with an internal error. Now, GDB handles the described scenario gracefully, reporting back to the user that the attach request failed. As a result, the user receives a warning noting that GDB was unable to attach because permission was denied. In addition, the debugging session is not affected by this behavior.

BZ#1186476

When a breakpoint was pending and a new object file appeared and this new object file contained multiple possible locations for the breakpoint, GDB was being too strict on checking this condition, and issued an internal error. The check for multiple locations for the same breakpoint has been relaxed, and GDB no longer issues an internal error in this scenario. The user now receives a warning mentioning that more than one location for the breakpoint has been found, but only one location will be used.

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

7.60. gdbm

7.60.1. RHBA-2015:0005 — gdbm bug fix update

Updated gdbm packages that fix one bug are now available for Red Hat Enterprise Linux 6.

Gdbm is a GNU database indexing library, which includes routines which use extensible hashing. Gdbm works in a similar way to standard UNIX dbm routines.

Bug Fix

BZ#629640

Due to incorrect open file flags, the gdbm utility caused creation of a new file when opening a non-existent file for reading. To fix this bug, the wrong file open flags have been set correctly, and gdbm thus no longer creates a new file in the aforementioned scenario.

Users of gdbm are advised to upgrade to these updated packages, which fix this bug.

7.60.2. RHBA-2015:0089 — gdbm bug fix update

Updated gdbm packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The gdbm packages provide a GNU database indexing library, which includes routines that use extensible hashing. The library works in a similar way to standard UNIX dbm routines.

Bug Fix

BZ#1180392

The previous release of gdbm introduced a regression in the way file handlers were used. Consequently, gdbm failed to write to a database opened for reading and writing. With this update, the file handlers have been fixed to use the right flags, and as a result, gdbm works with such databases as expected.

Users of gdbm are advised to upgrade to these updated packages, which fix this bug.

7.61. ghostscript

7.61.1. RHBA-2015:1343 — ghostscript bug fix update

Updated ghostscript packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The Ghostscript suite contains utilities for rendering PostScript and PDF documents. Ghostscript translates PostScript code to common, bitmap formats so that the code can be displayed or printed.

Bug Fixes

BZ#994452

Previously, a text intended for rendering in mode 3 (invisible) was not included in the PDF output of the pdfwrite device. As a consequence, text selection from documents with an invisible text, such as Optical character recognition (OCR) output, failed. With this update, mode 3 text is included in the PDF output, and copying a text from such PDF files now works as expected.

BZ#1027534

Prior to this update, some PDF files containing embedded objects were erroneously treated as portable collections, leading to a "/syntaxerror" error when processing these files. A fix has been applied so that only PDF files with "/Collection" attributes are treated as portable collections, and files with embedded objects are now processed correctly.

BZ#1060026

Correct PDF/A files could not be created due to a lack of support. This update backports improved support for creating PDF/A files from upstream, and correct PDF/A files can now be produced.

BZ#1105520

Previously, if an error occurred in the ghostscript interpreter in between allocating an array and initializing its contents, garbage collection could cause the interpreter to terminate unexpectedly while attempting to deallocate memory. A patch from upstream which immediately sets the array elements to null objects after allocation fixes this bug, and the ghostscript interpreter no longer crashes in the described scenario.

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

7.62. glibc

7.62.1. RHBA-2015:1286 — glibc bug fix and enhancement update

Updated glibc packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The glibc packages provide the standard C libraries (libc), POSIX thread libraries (libpthread), standard math libraries (libm), and the name server cache daemon (nscd) used by multiple programs on the system. Without these libraries, the Linux system cannot function correctly.

Bug Fixes

BZ#859965

This update of the name service cache daemon (nscd) adds a system of inotify-based monitoring and stat-based backup monitoring for nscd configuration files, so that nscd now correctly detects changes to its configuration and reloads the data. This prevents nscd from returning stale data.

BZ#1085312

A defect in the library could cause the list of returned netgroups to be truncated if one of the netgroups in the tree was empty. This error could result in application crashes or undefined behavior. The library has been fixed to handle empty netgroups correctly and to return the complete list of requested netgroups.

BZ#1088301

The gethostby* functions generated syslog messages for every unrecognized record type, even if the resolver options explicitly selected extra data. The library has been fixed to avoid generating logging messages when the user explicitly or implicitly requested the data. The number of syslog messages in DNSSEC-enabled systems related to calls to gethostby* is now reduced.

BZ#1091915

A defect in glibc could cause uninitialized bytes to be sent via a socket between the nscd client and server. When the application was analyzed using Valgrind, it reported a problem which could be confusing and misleading. The library has been fixed to initialize all bytes sent via the socket operation. Valgrind no longer reports problems with the nscd client.

BZ#1116050

A defect in the reinitialization of thread local structures could result in a too-small thread local storage structure which could lead to unexpected termination of an application. The thread library has been fixed to reinitialize the thread local storage structure correctly to prevent applications from crashing when they reuse thread stacks.

BZ#1124204

The times function provided by glibc did not allow users to use a NULL value for the buffer, and applications passing a NULL could terminate unexpectedly. The library has been fixed to accept a NULL value for the buffer and return the expected results from the kernel system call.

BZ#1138769

The getaddrinfo(3) function has been improved to return a valid response when an address lookup using the getaddrinfo(3) function for AF_UNSPEC is performed on a defective DNS server.

BZ#1159167

When using NetApp filers as NFS servers, the rpc.statd service could terminate unexpectedly. The glibc API segmentation violation in the server Remote Procedure Call (RPC) code that was causing this crash has been corrected, and the problem no longer occurs.

BZ#1217186

When a system with a large .rhosts file used the rsh shell to connect to a rlogind server, the authentication could time out. This update adjusts the ruserok(3) function, so that it first performs user matching in order to avoid demanding DNS lookups. As a result, rlogind authentication with large .rhosts files is faster and no longer times out.

Enhancements

BZ#1154563

The dlopen(3) function of the library, which is used to load dynamic libraries, can now be called recursively (a dlopen(3) function can be called while another dlopen(3) function is already in process). This update prevents crashes or aborts in applications that need to use the dlopen(3) function in this way.

BZ#1195453

The glibc dynamic loader now supports Intel AVX-512 extensions. This update allows the dynamic loader to save and restore AVX-512 registers as required, thus preventing AVX-512-enabled applications from failing because of audit modules that also use AVX-512.

Users of glibc are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.63. glusterfs

7.63.1. RHBA-2015:0683 — glusterfs bug fix update

Updated glusterfs packages that fix one bug are now available for Red Hat Enterprise Linux 6.

GlusterFS is a key building block of Red Hat Storage. It is based on a stackable user-space design and can deliver exceptional performance for diverse workloads. GlusterFS aggregates various storage servers over network interconnections into one large, parallel network file system.

Bug Fix

BZ#1204589

Previously, the qemu-kvm utility could terminate unexpectedly with a segmentation fault after the user attempted to create an image on GlusterFS using the "qemu-img create" command. The glusterfs packages source code has been modified to fix this bug, and qemu-kvm no longer crashes in the described situation.

Users of glusterfs are advised to upgrade to these updated packages, which fix this bug.

7.64. gnome-settings-daemon

7.64.1. RHBA-2015:0658 — gnome-settings-daemon bug fix update

Updated gnome-settings-daemon packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The gnome-settings-daemon packages contain a daemon to share settings from GNOME to other applications. It also handles global key bindings, as well as a number of desktop-wide settings.

Bug Fix

BZ#1098370

Due to a memory leak in the "housekeeping" plug-in, gnome-settings-daemon did not correctly release certain memory segments that were not needed anymore. Consequently, the daemon could possibly exhaust all available memory, in which case the system encountered performance issues. With this update, the "housekeeping" plug-in has been fixed to properly free unused memory. As a result, the above-mentioned scenario is prevented.

Users of gnome-settings-daemon are advised to upgrade to these updated packages, which fix this bug.

7.65. gnutls

7.65.1. RHSA-2015:1457 — Moderate: gnutls security and bug fix update

Updated gnutls packages that fix three security issues and one bug are now available for Red Hat Enterprise Linux 6.

Red Hat Product Security 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 GnuTLS library provides support for cryptographic algorithms and for protocols such as Transport Layer Security (TLS).

Security Fixes

CVE-2014-8155

It was found that GnuTLS did not check activation and expiration dates of CA certificates. This could cause an application using GnuTLS to incorrectly accept a certificate as valid when its issuing CA is already expired.

CVE-2015-0282

It was found that GnuTLS did not verify whether a hashing algorithm listed in a signature matched the hashing algorithm listed in the certificate. An attacker could create a certificate that used a different hashing algorithm than it claimed, possibly causing GnuTLS to use an insecure, disallowed hashing algorithm during certificate verification.

CVE-2015-0294

It was discovered that GnuTLS did not check if all sections of X.509 certificates indicate the same signature algorithm. This flaw, in combination with a different flaw, could possibly lead to a bypass of the certificate signature check.

The CVE-2014-8155 issue was discovered by Marcel Kolaja of Red Hat. The CVE-2015-0282 and CVE-2015-0294 issues were discovered by Nikos Mavrogiannopoulos of the Red Hat Security Technologies Team.

Bug Fix

BZ#1036385

Previously, under certain circumstances, the certtool utility could generate X.509 certificates which contained a negative modulus. Consequently, such certificates could have interoperation problems with the software using them. The bug has been fixed, and certtool no longer generates X.509 certificates containing a negative modulus.

Users of gnutls are advised to upgrade to these updated packages, which contain backported patches to correct these issues.

7.66. gpxe

7.66.1. RHEA-2015:1368 — gpxe enhancement update

Updated gpxe packages that add one enhancement are now available for Red Hat Enterprise Linux 6.

The gpxe package provides gPXE, an open source Pre-boot Execution Environment (PXE) implementation and boot loader.

Enhancement

BZ#968474

This update corrects the timeout values used by gPXE to conform to RFC 2131 and the PXE specification.

Users of gpxe are advised to upgrade to these updated packages, which add this enhancement.

7.67. grep

7.67.1. RHSA-2015:1447 — Low: grep security, bug fix, and enhancement update

Updated grep packages that fix two security issues, several bugs, and add various enhancements are now available for Red Hat Enterprise Linux 6.

Red Hat Product Security 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.

The grep utility searches through textual input for lines that contain a match to a specified pattern and then prints the matching lines. The GNU grep utilities include grep, egrep, and fgrep.

Security Fixes

CVE-2012-5667

An integer overflow flaw, leading to a heap-based buffer overflow, was found in the way grep parsed large lines of data. An attacker able to trick a user into running grep on a specially crafted data file could use this flaw to crash grep or, potentially, execute arbitrary code with the privileges of the user running grep.

CVE-2015-1345

A heap-based buffer overflow flaw was found in the way grep processed certain pattern and text combinations. An attacker able to trick a user into running grep on specially crafted input could use this flaw to crash grep or, potentially, read from uninitialized memory.

The grep packages have been upgraded to upstream version 2.20, which provides a number of bug fixes and enhancements over the previous version. Notably, the speed of various operations has been improved significantly. Now, the recursive grep utility uses the fts function of the gnulib library for directory traversal, so that it can handle much larger directories without reporting the "File name too long" error message, and it can operate faster when dealing with large directory hierarchies. (BZ#982215, BZ#1064668, BZ#1126757, BZ#1167766, BZ#1171806)

Bug Fixes

BZ#799863

Prior to this update, the \w and \W symbols were inconsistently matched to the [:alnum:] character class. Consequently, regular expressions that used \w and \W in some cases had incorrect results. An upstream patch which fixes the matching problem has been applied, and \w is now matched to the [_[:alnum:]] character and \W to the [^_[:alnum:]] character consistently.

BZ#1103270

Previously, the "--fixed-regexp" command-line option was not included in the grep(1) manual page. Consequently, the manual page was inconsistent with the built-in help of the grep utility. To fix this bug, grep(1) has been updated to include a note informing the user that "--fixed-regexp" is an obsolete option. Now, the built-in help and manual page are consistent regarding the "--fixed-regexp" option.

BZ#1193030

Previously, the Perl Compatible Regular Expression (PCRE) library did not work correctly when matching non-UTF-8 text in UTF-8 mode. Consequently, an error message about invalid UTF-8 byte sequence characters was returned. To fix this bug, patches from upstream have been applied to the PCRE library and the grep utility. As a result, PCRE now skips non-UTF-8 characters as non-matching text without returning any error message.

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

7.68. grub

7.68.1. RHBA-2015:1426 — grub bug fix update

Updated grub packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The grub packages provide Grand Unified Boot Loader (GRUB), a boot loader capable of booting a wide variety of operating systems.

Bug Fix

BZ#1177321, BZ#1206542

Previously, during the Pre-Boot Execution Environment (PXE) booting of a client configured to use the UEFI booting and the IP version 6 (IPv6) protocol, the client failed to display the expected selection menu as configured in the grub.cfg file and switched to the GRUB shell instead. With this update, the bug has been fixed so that the PXE boots the client and displays the operating system selection menu as configured in grub.cfg.

Users of grub are advised to upgrade to these updated packages, which fix this bug.

7.69. gstreamer-plugins-good

7.69.1. RHBA-2015:0666 — gstreamer-plugins-good bug fix update

Updated gstreamer-plugins-good packages that fix one bug are now available for Red Hat Enterprise Linux 6.

GStreamer is a streaming media framework based on graphs of filters which operate on media data. The gstreamer-plugins-good packages contain a collection of well-supported plug-ins of good quality and under the LGPL license.

Bug Fix

BZ#622776

Previously, using GStreamer with the Phonon back end, common in the K Desktop Environment (KDE), led to sound synchronization problems, which caused jitter in the audio output. With this update, the improperly working GStreamer component and the consequent sound synchronization problems have been fixed. As a result, sound quality in applications using Phonon is no longer affected.

Users of gstreamer-plugins-good are advised to upgrade to these updated packages, which fix this bug.

7.70. gvfs

7.70.1. RHBA-2015:0237 — gvfs bug fix update

Updated gvfs packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

GVFS is the GNOME Desktop Virtual File System layer that allows users to easily access local and remote data via File Transfer Protocol (FTP), Secure Shell File Transfer Protocol (SFTP), Web Distributed Authoring and Versioning (WebDAV), Common Internet File System (CIFS), Server Message Block (SMB), and other protocols. GVFS integrates with the GNOME I/O (GIO) abstraction layer.

Bug Fixes

BZ#998061

Previously, the GNOME Desktop Virtual File System (GVFS) trash implementation did not take access permissions into consideration when creating file monitors for mount points. Consequently, file monitors were polling files without read access permissions, preventing AutoFS mount points from expiring as they normally would when not in use for some time. With this update, the trash implementation no longer creates file monitors to monitor files without read access permissions. As a result, AutoFS mount points can now freely expire.

BZ#1140451

Prior to this update, gvfs-gdu-volume-monitor did not verify whether it received the data when getting the pool of GNOME Disk Utility (GDU) devices. Consequently, the gvfs-gdu-volume-monitor process could terminate unexpectedly if the data was not received. Now, gvfs-gdu-volume-monitor verifies whether the data was received, and no longer crashes.

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

7.70.2. RHBA-2015:1428 — gvfs bug fix update

Updated gvfs packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

GVFS is the GNOME Desktop Virtual File System layer that allows users to easily access local and remote data using File Transfer Protocol (FTP), Secure Shell File Transfer Protocol (SFTP), Web Distributed Authoring and Versioning (WebDAV), Common Internet File System (CIFS), Server Message Block (SMB), and other protocols. GVFS integrates with the GNOME I/O (GIO) abstraction layer.

Bug Fixes

BZ#1165676

Prior to this update, the gvfsd-gphoto2 utility did not verify whether it received the data when getting information on the camera attached storage. Consequently, gvfsd-gphoto2 could terminate unexpectedly if the data was not received. Now, gvfsd-gphoto2 verifies whether the data was received, and no longer crashes in the described situation.

BZ#1210203

The gvfsd-metadata daemon did not correctly handle the situation when an application tried to save a metadata entry larger than the size of a journal file, that is, larger than 32 kB. The daemon wrote all changes from the journal to the metadata database to make more space for the entry and then created a new journal file. This operation was repeated in an infinite loop unnecessarily, overloading the CPU and disk. With this update, the operation is retried only once. As a result, the metadata entry is not saved if it is too large, and gvfsd-metadata returns a warning instead.

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

7.71. hal-info

7.71.1. RHBA-2015:1268 — hal-info bug fix update

An updated hal-info package that fixes one bug and adds one enhancement is now available for Red Hat Enterprise Linux 6.

The hal-info package contains various device information files (also known as .fdi files) for the hal package.

Bug Fix

BZ#841419

Previously, the "Mic Mute" and "Touchpad Toggle" keys did not transmit the correct symbol in Lenovo laptops. With this update, the aforementioned keys are correctly recognized by the X.Org Server, and the XF86AudioMicMute and XF86TouchpadToggle signals are transmitted successfully.

Enhancement

BZ#1172669

To support the various "Fn" keys on latest Toshiba laptops, this update changes the hal-info remapping rules for Toshiba laptops from the provided kernel keycode to a keycode compatible with X.

Users of hal-info are advised to upgrade to this updated package, which fixes this bug and adds this enhancement.

7.72. haproxy

7.72.1. RHBA-2015:1400 — haproxy bug fix and enhancement update

Updated haproxy packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The haproxy packages provide a reliable, high-performance network load balancer for TCP and HTTP-based applications.

Upgrade to an upstream version

The haproxy packages have been upgraded to upstream version 1.5.4, which provides a number of bug fixes and enhancements over the previous version. (BZ#1136550)

Enhancement

BZ#1166497

The OPTIONS parameter has been added to the /etc/sysconfig/haproxy file, which allows the user to set extra options for the haproxy utility.

Users of haproxy are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.73. hivex

7.73.1. RHSA-2015:1378 — Moderate: hivex security and bug fix update

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

Red Hat Product Security 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.

Hivex is a library that can read and write Hive files, undocumented binary files that Windows uses to store the Windows Registry on disk.

Security Fix

CVE-2014-9273

It was found that hivex attempted to read, and possibly write, beyond its allocated buffer when reading a hive file with a very small size or with a truncated or improperly formatted content. An attacker able to supply a specially crafted hive file to an application using the hivex library could possibly use this flaw to execute arbitrary code with the privileges of the user running that application.

Red Hat would like to thank Mahmoud Al-Qudsi of NeoSmart Technologies for reporting this issue.

Bug Fix

BZ#1164693

The hivex(3) man page previously contained a typographical error. This update fixes the typo.

Red Hat would like to thank Mahmoud Al-Qudsi of NeoSmart Technologies for reporting this issue.

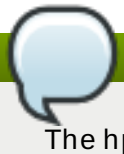
All hivex users are advised to upgrade to these updated packages, which contain backported patches to correct these issues.

7.74. hplip

7.74.1. RHBA-2015:1282 — hplip bug fix and enhancement update

Updated hplip packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The hplip packages contain the Hewlett-Packard Linux Imaging and Printing Project (HPLIP), which provides drivers for Hewlett-Packard printers and multi-function peripherals.



Upgrade to an upstream version

The hplip packages have been upgraded to upstream version 3.14.6, which provides a number of bug fixes and enhancements over the previous version, including hardware enablement and new functionality, such as the Service Location Protocol (SLP) discovery feature. (BZ#1077121)

Bug Fixes

BZ#682814

Previously, HPLIP did not correctly handle CUPS denying a requested operation, such enabling or disabling a printer. As a consequence, operating HP Device Manager as a non-root user did not prompt for the root password when the root password was required for an operation. With this update, the password callback is correctly implemented, and operating HP Device Manager as non-root user now always prompts for the root password when required.

BZ#876066

Prior to this update, the use of an uninitialized value could produce incorrect output from the hpcups driver. The underlying source code has been modified to initialize the value before it is used, and the described unexpected behavior is therefore prevented.

Users of hplip are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.75. httpd

7.75.1. RHSA-2015:1249 — Low: httpd security, bug fix, and enhancement update

Updated httpd packages that fix one security issue, several bugs, and add one enhancement are now available for Red Hat Enterprise Linux 6.

Red Hat Product Security 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 httpd packages provide the Apache HTTP Server, a powerful, efficient, and extensible web server.

Security Fix

CVE-2013-5704

A flaw was found in the way httpd handled HTTP Trailer headers when processing requests using chunked encoding. A malicious client could use Trailer headers to set additional HTTP headers after header processing was performed by other modules. This could, for example, lead to a bypass of header restrictions defined with mod_headers.

Bug Fixes

BZ#1149906

The order of mod_proxy workers was not checked when httpd configuration was reloaded. When mod_proxy workers were removed, added, or their order was changed, their parameters and scores could become mixed. The order of mod_proxy workers has been made internally consistent during configuration reload.

BZ#906476

The local host certificate created during firstboot contained CA extensions, which caused the httpd service to return warning messages. This has been addressed by local host certificates being generated with the "-extensions v3_req" option.

BZ#1086771

The default mod_ssl configuration no longer enables support for SSL cipher suites using the single DES, IDEA, or SEED encryption algorithms.

BZ#963146

The apachectl script did not take into account the HTTPD_LANG variable set in the /etc/sysconfig/httpd file during graceful restarts. Consequently, httpd did not use a changed value of HTTPD_LANG when the daemon was restarted gracefully. The script has been fixed to handle the HTTPD_LANG variable correctly.

BZ#1057695

The mod_deflate module failed to check the original file size while extracting files larger than 4 GB, making it impossible to extract large files. Now, mod_deflate checks the original file size properly according to RFC1952, and it is able to decompress files larger than 4 GB.

BZ#1146194

The httpd service did not check configuration before restart. When a configuration contained an error, an attempt to restart httpd gracefully failed. Now, httpd checks configuration before restart and if the configuration is in an inconsistent state, an error message is printed, httpd is not stopped and a restart is not performed.

BZ#1149703

The SSL_CLIENT_VERIFY environment variable was incorrectly handled when the "SSLVerifyClient optional_no_ca" and "SSLSessionCache" options were used. When an SSL session was resumed, the SSL_CLIENT_VERIFY value was set to "SUCCESS" instead of the previously set "GENEROUS". SSL_CLIENT_VERIFY is now correctly set to GENEROUS in this scenario.

BZ#1045477

The ab utility did not correctly handle situations when an SSL connection was closed after some data had already been read. As a consequence, ab did not work correctly with SSL servers and printed "SSL read failed" error messages. With this update, ab works as expected with HTTPS servers.

BZ#1161328

When a client presented a revoked certificate, log entries were created only at the debug level. The log level of messages regarding a revoked certificate has been increased to INFO, and administrators are now properly informed of this situation.

Enhancement

BZ#767130

A mod_proxy worker can now be set into drain mode (N) using the balancer-manager web interface or using the httpd configuration file. A worker in drain mode accepts only existing sticky sessions destined for itself and ignores all other requests. The worker waits until all clients currently connected to this worker complete their work before the worker is stopped. As a result, drain mode enables to perform maintenance on a worker without affecting clients.

Users of httpd are advised to upgrade to these updated packages, which contain backported patches to correct these issues and add this enhancement. After installing the updated packages, the httpd service will be restarted automatically.

7.76. hwdata

7.76.1. RHEA-2015:1349 — hwdata enhancement update

An updated hwdata package that adds one enhancement is now available for Red Hat Enterprise Linux 6.

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

Enhancement

BZ#1170975

The PCI, USB, and vendor ID files have been updated with information about recently released hardware. Hardware utility tools that use these ID files are now able to correctly identify recently released hardware.

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

7.77. hyperv-daemons

7.77.1. RHBA-2015:1311 — hyperv-daemons bug fix update

Updated hyperv-daemons packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The hyperv-daemons packages provide a suite of daemons that are needed when a Red Hat Enterprise Linux guest is running on Microsoft Hyper-V. The following daemons are included: - hypervkvpd, the guest Hyper-V Key-Value Pair (KVP) daemon - hypervvssd, the implementation of Hyper-V VSS functionality - hypervfcopyd, the implementation of Hyper-V file copy service functionality

Bug Fix

BZ#1161368

When mounting a read-only file system that does not support file system freezing (such as SquashFS) and using the online backup feature, the online backup previously failed with an "Operation not supported" error. This update fixes the hypervvssd daemon so that it handles the online backup correctly, and the described error no longer occurs.

Users of hyperv-daemons are advised to upgrade to these updated packages, which fix this bug.

7.78. ibus

7.78.1. RHBA-2015:0657 — ibus bug fix update

Updated ibus packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The Intelligent Input Bus (IBus) is an input method framework for multilingual input in Unix-like operating systems.

Bug Fixes

BZ#1066075

Previously, Java applications generated by Lotus Sametime or Eclipse became unresponsive when the Korean language input engine platform for the IBus input method (ibus-hangul) was used in Red Hat Enterprise Linux 6. To fix this bug, asynchronous key events have been added to IBus. Now, IBus can switch to asynchronous mode which resolves the hang.

BZ#1043381

Prior to this update, the X11 application became unresponsive when the user was typing using IBus and switched input contexts between the parent and the child windows. This update resolves the race condition causing this bug. Now, IBus properly handles the situation and the application no longer hangs.

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

7.79. icu

7.79.1. RHEA-2015:1438 — icu enhancement update

Updated icu packages that add one enhancement are now available for Red Hat Enterprise Linux 6.

The International Components for Unicode (ICU) library provides robust and full-featured Unicode services.

Enhancement

BZ#1200973

Transliteration from Latin to US-ASCII characters is now supported. Prior to this update, icu in Red Hat Enterprise Linux 6 did not support this mode of the transliterator_transliterate() function. Consequently, it was not possible to perform certain operations. For example, the user could not easily remove non-ASCII characters from PHP code strings. With this update, the user can use transliterator_transliterate() to transliterate Latin characters to US-ASCII characters.

Users of icu are advised to upgrade to these updated packages, which add this enhancement.

7.79.2. RHBA-2015:0664 — icu bug fix update

Updated icu packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The International Components for Unicode (ICU) library provides robust and full-featured Unicode services.

Bug Fix

BZ#1176177

Previously, during the rebuild process of the icu source package, two-digit format was used for calendar year in the test case and was not interpreted correctly. As a consequence, the year 2034 was displayed instead of year 1934 causing the check of the test case to fail. A patch has been applied to fix this bug and the check no longer fails.

Users of icu are advised to upgrade to these updated packages, which fix this bug.

7.80. initscripts

7.80.1. RHBA-2015:1380 — initscripts bug fix update

Updated initscripts packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The initscripts packages contain basic system scripts to boot the system, change runlevels, activate and deactivate most network interfaces, and shut down the system cleanly.

Bug Fixes

BZ#1129624

Due to a race condition, the multicast_snooping bridging option failed to be applied before creating a bridge device. With this update, multicast_snooping is applied after the bridge is up, and the option now works as intended.

BZ#957706

Previously, the rc.sysinit script only set affinity for PID 1 (init), which caused that processes that were run from sysinit did not inherit this setting. This update sets affinity also for the script itself, and thus initscripts correctly set affinity for all running processes.

BZ#919472

The net.bridge.bridge-nf-call-ip6tables key was previously applied on all systems. Consequently, when a kernel module was missing, harmless but unnecessary messages were returned. The rules have been relocated from sysctl.conf, which ensures that they are applied only if needed.

BZ#1101546

When a shutdown was attempted while an NFS Client machine had I/O in progress on an NFS mount, the system became unresponsive during shutdown. This update applies a lazy mount, within which all processes that have open File Descriptors (FDs) are found and killed, and hangs thus no longer occur in this situation.

BZ#1136863

Previously, the netconsole starting priority was set to 50, which caused that netconsole was started late during the system boot. This update lowers the priority so that netconsole starts right after the network is up.

BZ#1157816

If resolv.conf.save was present, resolv.conf was overwritten by the content of resolv.conf.save. As a consequence, unexpected changes could occur to resolve.conf. Now, the content of resolv.conf is replaced only when the device is dynamically configured or contains DNS options in its ifcfg file.

BZ#997271

Previously, the broadcast address was not computed correctly due to the ipcalc utility not being aware of RFC 3021. With this update, ipcalc correctly recognizes RFC 3021, thus fixing this bug.

BZ#1109588

Previously, network aliases did not inherit the ARPCHECK variable from their parents, which

caused that parents where not checked for duplicate IP addresses but their aliases did check them. With this update, alias devices inherit ARPCHECK.

BZ#1164902

Previously, a syntax error occurred when using the tcsh shell along with the grep utility, returning the following error after logging:

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

The lang.csh code has been fixed, and error messages are no longer returned in this scenario.

BZ#1168664

Prior to this update, if the system became unresponsive during boot, the administrator was not able to determine the cause. This update adds more informative messages returned by rc.sysinit. In addition, a new rc.debug option for the kernel command line has been added, so that the administrator receives proper debugging information.

BZ#1176999

Due to a syntax error in the install_bonding_driver() function, the following error message was returned:

/sys/class/net/bonding/slaves: No such file or directory

The syntax error has been fixed, and the aforementioned error message is no longer returned.

BZ#1189337

Previously, network initscripts silently failed if the root was on the network file system and did not perform any action, which was confusing. Now, network initscripts print the following message to inform the system administrator:

rootfs is on network filesystem, leaving network up

BZ#1072967

Previously, the "ip addr flush" command was called with global scope, which is incorrect for loopback addresses. Consequently, the system could become unresponsive. With this update, the scope host for loopback is used, and the flush operation works as expected.

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

7.81. ipa

7.81.1. RHSA-2015:1462 — Moderate: ipa security and bug fix update

Updated ipa packages that fix two security issues and several bugs are now available for Red Hat Enterprise Linux 6.

Red Hat Product Security 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.

Red Hat Identity Management (IdM) is a centralized authentication, identity management, and authorization solution for both traditional and cloud-based enterprise environments.

Two cross-site scripting (XSS) flaws were found in jQuery, which impacted the Identity Management web administrative interface, and could allow an authenticated user to inject arbitrary HTML or web script into the interface. (CVE-2010-5312, CVE-2012-6662)

Bug Fixes

BZ#1131571

The ipa-server-install, ipa-replica-install, and ipa-client-install utilities are not supported on machines running in FIPS-140 mode. Previously, IdM did not warn users about this. Now, IdM does not allow running the utilities in FIPS-140 mode, and displays an explanatory message.

BZ#1132261

If an Active Directory (AD) server was specified or discovered automatically when running the ipa-client-install utility, the utility produced a traceback instead of informing the user that an IdM server is expected in this situation. Now, ipa-client-install detects the AD server and fails with an explanatory message.

BZ#1154687

When IdM servers were configured to require the TLS protocol version 1.1 (TLSv1.1) or later in the httpd server, the ipa utility failed. With this update, running ipa works as expected with TLSv1.1 or later.

BZ#1161722

In certain high-load environments, the Kerberos authentication step of the IdM client installer can fail. Previously, the entire client installation failed in this situation. This update modifies ipa-client-install to prefer the TCP protocol over the UDP protocol and to retry the authentication attempt in case of failure.

BZ#1185207

If ipa-client-install updated or created the /etc/nsswitch.conf file, the sudo utility could terminate unexpectedly with a segmentation fault. Now, ipa-client-install puts a new line character at the end of nsswitch.conf if it modifies the last line of the file, fixing this bug.

BZ#1191040

The ipa-client-automount utility failed with the "UNWILLING_TO_PERFORM" LDAP error when the nsslapd-minssf Red Hat Directory Server configuration parameter was set to "1". This update modifies ipa-client-automount to use encrypted connection for LDAP searches by default, and the utility now finishes successfully even with nsslapd-minssf specified.

BZ#1198160

If installing an IdM server failed after the Certificate Authority (CA) installation, the "ipa-server-install --uninstall" command did not perform a proper cleanup. After the user issued "ipa-server-install --uninstall" and then attempted to install the server again, the installation failed. Now, "ipa-server-install --uninstall" removes the CA-related files in the described situation, and ipa-server-install no longer fails with the mentioned error message.

BZ#1198339

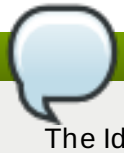
Running ipa-client-install added the "sss" entry to the sudoers line in nsswitch.conf even if "sss" was already configured and the entry was present in the file. Duplicate "sss" then caused sudo to become unresponsive. Now, ipa-client-install no longer adds "sss" if it is already present in nsswitch.conf.

BZ#1201454

After running ipa-client-install, it was not possible to log in using SSH under certain circumstances. Now, ipa-client-install no longer corrupts the sshd_config file, and the sshd service can start as expected, and logging in using SSH works in the described situation.

BZ#1220788

An incorrect definition of the dc attribute in the /usr/share/ipa/05rfc2247.ldif file caused bogus error messages to be returned during migration. The attribute has been fixed, but the bug persists if the copy-schema-to-ca.py script was run on Red Hat Enterprise Linux 6.6 prior to running it on Red Hat Enterprise Linux 6.7. To work around this problem, manually copy /usr/share/ipa/schema/05rfc2247.ldif to /etc/dirsrv/slapd-PKI-IPA/schema/ and restart IdM.



Note

The IdM version provided by this update no longer uses jQuery.

All ipa users are advised to upgrade to these updated packages, which contain backported patches to correct these issues.

7.82. ipmitool

7.82.1. RHBA-2015:1351 — ipmitool bug fix update

Updated ipmitool packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The ipmitool packages contain a command-line utility for interfacing with devices that support the Intelligent Platform Management Interface (IPMI) specification. IPMI is an open standard for machine health, inventory, and remote power control.

Bug Fixes

BZ#878614

Prior to this update, ipmitool could handle only 16-byte-long Sensor Data Repository (SDR) item names. Consequently, listing a sensor with a long name could cause ipmitool to terminate unexpectedly. This update fixes the string identification handling, and the long sensor names are now trimmed correctly.

BZ#903019

Previously, ipmitool could not recognize neither sensor thresholds and presence, nor fan units of sensors on Sun Fire X4600 M2 Servers. This update resolves the unrecognized sensor reporting.

BZ#1028163

Previously, the ipmitool default timeout values set an insufficient time period. As a consequence, during retries, ipmitool could terminate unexpectedly with a segmentation fault, or produce a nonsensical error message. With this update, the ipmitool options passed from the environment variable are parsed correctly from the IPMITOOL_OPTS and IPMI_OPTS variables, and IPMITOOL_* variables take precedence over IPMI_* variables. As a result, ipmitool no longer crashes in the described situation.

BZ#1126333

Previously, ipmitool could not recognize the Sensor Data Repository (SDR) type Software ID. As a consequence, the default 5-second timeout for each affected line reported resulted in a very slow response. This update fixes the Intelligent Platform Management Bus (IPMB) request setup, and slow SDR access times are no longer experienced in the described situation.

BZ#1162175

Previously, the ipmitool utility required an unnecessary dependency on the OpenIPMI packages, which had to be installed together with ipmitool. This update removes the dependency on the OpenIPMI packages, which are no longer installed when installing ipmitool.

BZ#1170266

An earlier version of ipmitool contained a version mismatch between the ipmitool packages and the runtime-reported version. Consequently, running the "ipmitool -V" command displayed the 1.8.14 version number instead of the correct 1.8.11 version number. With this update, the runtime version change has been reverted to match the package version.

BZ#1194420

Previously, ipmitool could not recognize DDR4 memory modules and could terminate unexpectedly with a segmentation fault on such systems. This update adds support for DDR4 reporting. As a result, ipmitool no longer crashes on DDR4 systems when running the Field Replacement Unit (FRU) inventory listing.

Users of ipmitool are advised to upgrade to these updated packages, which fix these bugs. After installing this update, the IPMI event daemon (ipmievd) will be restarted automatically.

7.83. iproute

7.83.1. RHBA-2015:1331 — iproute bug fix and enhancement update

Updated iproute packages that fix several bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

The iproute packages contain networking utilities such as ip and rtmon designed to use the advanced networking capabilities of the Linux kernel.

Bug Fixes

BZ#997965

The default route was erroneously deleted after running the "ip route del" command without further parameters. A patch has been applied, and the default route is no longer removed in this situation.

BZ#1011817

Running the "bridge monitor file" command opened the file, but never closed it. A fix has been applied to close the opened file after loading its content. As a result, the command now closes all opened files as expected.

BZ#1034049

Previously, the "ip -6 addrlabel" command returned an incorrect error message that contained "inet" instead of "inet6". To fix this bug, the error message has been changed to include "inet" for IPv4 addresses and "inet6" for IPv6 addresses.

BZ#1040367

Prior to this update, the iproute utility handled the return values of the send() system call incorrectly when reading kernel responses. Consequently, iproute could interpret successful kernel responses as failures, which caused iproute to terminate with an error. With this update, iproute uses the return values correctly and processes kernel responses as intended.

BZ#1060195

The /sbin/ip file displayed statistics for 32-bit system even on 64-bit kernel. To fix this bug, a patch has been applied, and the statistics are now presented correctly.

BZ#1152951

Prior to this update, multipath routing did not function with IPv6 addresses and resulted in an "IP address is expected rather than "2001:470:25:94::1" error. To fix this bug, a patch that enables adding multipath routes using IPv6 addresses has been applied.

Enhancements

BZ#1131650

Support for spoof checking configuration has been added to iproute.

BZ#1177982

Dynamic precision, human readable, and IEC outputs are now backported to IP statistics.

Users of iproute are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.84. iprutils

7.84.1. RHBA-2015:1305 — iprutils bug fix and enhancement update

Updated iprutils packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The iprutils packages provide utilities to manage and configure Small Computer System Interface (SCSI) devices that are supported by the ipr SCSI storage device driver.

Upgrade to an upstream version

The iprutils packages have been upgraded to upstream version 2.4.5, which provides a number of bug fixes and enhancements over the previous version. Notably, this update adds support for reporting cache hits on the Serial Attached SCSI (SAS) disk drive, and increases the speed of array creation for an advanced function (AF) direct-access storage device (DASD). (BZ#1148147)

Bug Fix

BZ#1146701

Previously, the format of firmware files was case sensitive. As a consequence, device attributes were not saved correctly for SIS-64 adapters after updating firmware with the pci.xxx file format. With this update, the firmware format is case insensitive, and device attributes are saved correctly in the described situation.

Users of iprutils are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.85. ipset

7.85.1. RHBA-2015:1353 — ipset bug fix update

Updated ipset packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The ipset packages provide IP sets, a framework inside the Linux 2.4.x and 2.6.x kernel, which can be administered by the ipset utility. Depending on the type, an IP set can currently store IP addresses, TCP/UDP port numbers or IP addresses with MAC addresses in a way that ensures high speed when matching an entry against a set.

Bug Fix

BZ#1121665

When the user was trying to create a program using the ipset library, linking failed with an undefined reference to the ipset_port_usage() function. With this update, ipset_port_usage() is now provided by the library and a program using the ipset library is now compiled successfully.

Users of ipset are advised to upgrade to these updated packages, which fix this bug.

7.86. iptables

7.86.1. RHBA-2015:1404 — iptables bug fix and enhancement update

Updated iptables packages that fix several bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

The iptables utility controls the network packet filtering code in the Linux kernel.

Bug Fixes

BZ#1081422

Previously, no iptables revision was used for rules that match an ipset. As a consequence, iptables rules with the match-set option could be added, but not removed again, as the rules could not be located again for their removal. This update adds revision 0 and 1 code patches for libipt_SET. As a result, new ipset match rules can now be removed. Please note that adding and removing rules using the match-set option now works with the patch applied, but removing a rule that was added with an earlier version of iptables does not work and cannot be fixed. Use the rule number to remove such rules.

BZ#1088400

In iptables version 1.4.7-9, the use of alternatives was introduced. Because of the use of

versioned (/lib*/xtables-%{version}) custom plug-ins, the plug-ins had to be placed in the appropriate versioned plug-in directory. Starting with iptables version 1.4.7-10, the plug-in directory was reverted back to /lib*/xtables/, but custom plug-ins from iptables version 1.4.7-9 were not copied over. Consequently, upgrading iptables 1.4.7-9 to a newer version led to a loss of custom plug-ins. A plug-in update trigger which detects updates to iptables from version 1.4.7-15 and lower has been added. As a result, custom plug-ins from the /%{_lib}/xtables-1.4.7/ directory are copied to the /%{_lib}/xtables/ directory if the plug-in in /%{_lib}/xtables-1.4.7/ has a newer file date or if it does not exist in the destination directory while updating from iptables version earlier than 1.4.7-15 to a newer version.

BZ#1084974

Previously, a space after Datagram Congestion Control Protocol (DCCP) packet types for print and save was missing, which led to malformed output. With this update, a space has been added at the end of the print_types() function output. As a result, the output of the "iptables -L", "iptables -S", and iptables-save commands is now correct.

BZ#1081191

Previously, some init script warning messages for a failed euid 0 check (no configuration file and nothing to save) were missing. Consequently, only exit status codes were provided in these cases, but no messages. This update adds the warning messages that are now provided in the described situation.

Enhancements

BZ#1161330

This update adds support for IPv6 ipset, as ipsets were not previously usable in IPv6 firewall rules.

BZ#1088361

This update adds support for the "-C" check option for the ip*tables commands. Previously, there was no simple way to check if a certain rule exists. Now, the "-C" option can be used in a rule to check if a rule exists.

Users of iptables are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.87. iputils

7.87.1. RHBA-2015:1251 — iputils bug fix update

Updated iputils packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The iputils packages contain basic utilities for monitoring a network, including ping.

Bug Fixes

BZ#829998

The arping command previously returned incorrect exit codes in some cases due to incorrect time related logic and exit-handling conditions in the code. With this update, the aforementioned problems have been fixed, and arping again returns correct values.

BZ#1099426

Due to incorrect code that handles the number of return path hops, the tracepath utility displayed an incorrect number of "back" hops. This update fixes the logic, and the number of displayed back hops is now accurate.

BZ#1113082

When domain name translation was forced to be carried out over the IPv6 protocol, the output of the "ping" command was incorrect as it displayed an incorrect IP address received from the internal library. The underlying logic has been modified to use the gethostbyname2() function instead of gethostbyname(), and domain name to IP address translation now works correctly.

BZ#1149574

Due to invalid logic present in the code, an erroneous warning message could be returned under certain circumstances:

WARNING: kernel is not very fresh, upgrade is recommended.

This update removes the code responsible for returning this erroneous warning message, thus fixing the bug.

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

7.88. irqbalance

7.88.1. RHBA-2015:1279 — irqbalance bug fix and enhancement update

Updated irqbalance packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The irqbalance packages provide a daemon that evenly distributes the interrupt request (IRQ) load across multiple CPUs for enhanced performance.

Upgrade to an upstream version

The irqbalance packages have been upgraded to upstream version 1.0.7, which provides a number of bug fixes and enhancements over the previous version. Notably, irqbalance now works with Xen PV guest, broken deepest cache backport has been fixed, and the IRQ migration algorithm has been enhanced. (BZ#1181720)

Bug Fixes

BZ#1158932

Previously, the irqbalance utility did not set signal handlers for particular signals. Consequently, when irqbalance received a signal other than SIGINT or SIGHUP, it terminated without a cleanup. This update provides signal handlers for SIGUSR1, SIGUSR2, and SIGTERM. As a result, irqbalance now stops gracefully after finishing the current balancing iteration.

BZ#1178247

Prior to this update, the /sys/bus/pci/devices file handle was not freed properly if the directory was not available. As a consequence, a memory leak occurred. With this update, the file handle is freed as expected when irqbalance cannot open the directory, and memory

the file handle is freed as expected when irqbalance cannot open the directory, and memory leaks no longer occur in the described situation.

Users of irqbalance are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.89. iscsi-initiator-utils

7.89.1. RHEA-2015:1371 — iscsi-initiator-utils enhancement update

Updated iscsi-initiator-utils packages that add one enhancement are now available for Red Hat Enterprise Linux 6.

The iscsi-initiator-utils packages provide the server daemon for the Internet Small Computer System Interface (iSCSI) protocol, as well as the utility programs used to manage it. The iSCSI protocol is a protocol for distributed disk access using SCSI commands sent over Internet Protocol (IP) networks.

Enhancement

BZ#691746

The Internet Small Computer System Interface (iSCSI) now supports safe logout. Previously, an iSCSI session was allowed to log out even when an iSCSI device was still mounted, which could cause the host to become unresponsive. This update adds the "iscsi.safe_logout" option. With "iscsi.safe_logout" set to "Yes" in the /etc/iscsi/iscsid.conf file, the system blocks attempts to log out of an iSCSI session when one or more connected iSCSI drives are mounted.

Users of iscsi-initiator-utils are advised to upgrade to these updated packages, which add this enhancement.

7.90. java-1.7.0-openjdk

7.90.1. RHEA-2015:1245 — java-1.7.0-openjdk bug fix and enhancement update

Updated java-1.7.0-openjdk packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The java-1.7.0-openjdk packages provide the OpenJDK 7 Java Runtime Environment and the OpenJDK 7 Java Software Development Kit for compiling and executing Java programs.

Bug Fixes

BZ#1145848

The TLS/SSL implementation in OpenJDK previously failed to handle Diffie-Hellman (DH) keys with more than 1024 bits. This caused client applications using Java Secure Socket Extension (JSSE) to fail to establish TLS/SSL connections to servers using larger DH keys during the connection handshake. This update adds support for DH keys with size up to 2048 bits, thus fixing this bug.

BZ#1146622

Previously, the OpenJDK utility displayed characters containing the umlaut diacritical mark (such as ä, ö, or ü) and the eszett character (ß) in PostScript output incorrectly. A patch with support for umlaut and eszett characters has been applied, and OpenJDK now displays these characters correctly.

BZ#1164762

The jhat man page URL was broken. A patch has been applied to fix this bug, and the URL now functions as expected.

BZ#1168693

Previously, it was not possible to use the Serviceability Agent (SA) tool when the target application contained symbols using non-ASCII characters. Java Virtual Machine (JVM) and SA calculated different hashes for strings with such characters, and SA terminated with an error. A patch has been applied to fix this bug, and SA no longer crashes when non-ASCII characters are used.

BZ#1173326

Previously, jvmtiStringPrimitiveCallback was invoked when a string value was null. Consequently, Java Virtual Machine (JVM) could terminate unexpectedly. A patch has been applied to fix this bug, and JVM no longer crashes in this situation.

BZ#1176718

Prior to this update, the Java Native Interface (JNI) code handling fonts used an incorrect function parameter when setting context. Consequently, Java Virtual Machine (JVM) could terminate unexpectedly when disposing of certain fonts. The use of function parameters by the JNI code has been amended, and JVM no longer crashes in this situation.

BZ#1190835

Previously, calling the Files.probeContentType() function with the default GnomeFileTypeDetector using the libgio library caused Java Virtual Machine (JVM) to terminate unexpectedly at a thread's end. A patch has been applied, and the process now exits without problems.

BZ#1214835

Due to a regression, the Java Heap/CPU Profiling Tool (HPROF) produced truncated output when used with the "doe=n" argument. Consequently, the output file contained only the header, the data was missing. A patch has been applied, and the output of HPROF is now correct when using "doe=n".

Enhancement

BZ#1121211

Support for elliptic curve cryptography, the SunEC provider, has been added to OpenJDK 7. OpenJDK 7 can now establish Transport Layer Security or Secure Sockets Layer connections or perform encryption and decryption using this technology.

Users of java-1.7.0-openjdk are advised to upgrade to these updated packages, which fix these bugs and add this enhancement. All running instances of OpenJDK Java must be restarted for the update to take effect.

7.91. java-1.8.0-openjdk

7.91.1. RHBA-2015:1427 — java-1.8.0-openjdk bug fix and enhancement update

Updated java-1.8.0-openjdk packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The java-1.8.0-openjdk packages contain the latest version of the Open Java Development Kit (OpenJDK), OpenJDK 8. These packages provide a fully compliant implementation of Java SE 8.

Bug Fixes

BZ#1154143

In Red Hat Enterprise Linux 6, the java-1.8.0-openjdk packages mistakenly included the SunEC provider, which does not function properly on this system. With this update, SunEC has been removed from the Red Hat Enterprise Linux 6 version of java-1.8.0-openjdk.

BZ#1155783

Prior to this update, the java-1.8.0-openjdk packages incorrectly provided "java-devel", which could lead to their inclusion in inappropriate builds. As a consequence, the "yum install java-devel" command in some cases installed java-1.8.0-openjdk-devel instead of the intended Java package. This update removes the providing configuration, and java-1.8.0-openjdk-devel can now be installed only by using the "yum install java-1.8.0-openjdk-devel" command.

BZ#1182011

Previously, the OpenJDK utility displayed characters containing the umlaut diacritical mark (such as ä, ö, or ü) and the eszett character (ß) in PostScript output incorrectly. A patch with support for umlaut and eszett characters has been applied, and OpenJDK now displays these characters correctly.

BZ#1189853

The java-1.8.0-openjdk package for Red Hat Enterprise Linux 6 did not provide the "java" virtual package. Consequently, when a package needed to use OpenJDK 8, it was necessary to require "java-1.8.0-openjdk" instead of commonly used "java". Now, it is sufficient to require "java" as expected.

BZ#1212592

OpenJDK used a copy of the system time zone data. This could cause a difference between OpenJDK time and the system time. Now, OpenJDK uses the system time zone data, and OpenJDK time and the system time are the same.

Enhancement

BZ#1210007

Red Hat now provides debug builds of OpenJDK in optional channels. With installed debug builds and JVM or JDK switched to using them, it is possible to do detailed HotSpot debugging. The debug builds can be used via alternatives or direct execution, in the same way as regular Java builds. Note that debug builds are not suitable for use in production, as they operate at a slower rate.

Users of java-1.8.0-openjdk are advised to upgrade to these updated packages, which fix these bugs and add this enhancement. All running instances of OpenJDK Java must be restarted for the update to take effect.

7.92. jpackage-utils

7.92.1. RHEA-2015:1248 — jpackage-utils enhancement update

An updated jpackage-utils package that adds one enhancement is now available for Red Hat Enterprise Linux 6.

The jpackage-utils package installs directory structures, RPM macros, configuration files, and scripts that provide support for jpackage.org Java packaging. It is required by all packages that follow the JPackage conventions.

Enhancement

BZ#1149605

The support for OpenJDK8 has been added to the JPackage utilities, which enables Java system applications to be used with OpenJDK8.

Users of jpackage-utils are advised to upgrade to this updated package, which adds this enhancement.

7.93. json-c

7.93.1. RHBA-2015:1397 — json-c bug fix update

Updated json-c packages that fix one bug are now available for Red Hat Enterprise Linux 6.

JSON-C implements a reference counting object model that allows users to easily construct JavaScript Object Notation (JSON) objects in C, output them as JSON formatted strings, and parse JSON formatted strings back into the C representation of JSON objects.

Bug Fix

BZ#1158842

The pkg-config (.pc) files for JSON-C were incorrectly placed in the /lib64/pkgconfig/ directory in the 64-bit packages and in the /lib/pkgconfig/ directory in the 32-bit packages. Consequently, the pkg-config tool was unable to find these files and failed to provide the location of the installed JSON-C libraries, header files, and other information about JSON-C. With this update, the pkg-config files have been moved to the /usr/lib64/pkgconfig/ and /usr/lib/pkgconfig/ directory respectively. As a result, the pkg-config tool now successfully returns information about the installed JSON-C packages.

Users of JSON-C are advised to upgrade to these updated packages, which fix this bug.

7.94. jss

7.94.1. RHBA-2015:1315 — jss bug fix and enhancement update

Updated jss packages that fix two bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

Java Security Services (JSS) provides an interface between Java Virtual Machine and Network Security Services (NSS). It supports most of the security standards and encryption technologies supported by NSS including communication through SSL/TLS network protocols. JSS is primarily utilized by the Certificate Server as a part of the Identity Management System.

Bug Fixes

BZ#1190302

Previously, the HASH_ALGORITHM constant was defined incorrectly. As a consequence, object identifiers (OIDs) for SHA-256, SHA-384, and SHA-512 hash functions were incorrect. With this update, the underlying source code has been modified, and the mentioned OIDs are now correct.

BZ#1190303

Prior to this update, the source code for JSS was missing a condition for validating the key strength for the RC4 software stream cipher. As a consequence, JSS did not validate the key strength properly. A patch has been applied to fix this bug, and JSS now performs key strength validation checks as expected.

Enhancement

BZ#1167470

The Tomcat service has been updated to support the Transport Layer Security cryptographic protocol version 1.1 (TLSv1.1) and the Transport Layer Security cryptographic protocol version 1.2 (TLSv1.2) using JSS.

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

7.95. kernel

7.95.1. RHSA-2015:1272 — Moderate: kernel security, bug fix, and enhancement update

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 6. This is the seventh regular update.

Red Hat Product Security 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.

Security Fixes

CVE-2014-3940, Moderate

A flaw was found in the way Linux kernel's Transparent Huge Pages (THP) implementation handled non-huge page migration. A local, unprivileged user could use this flaw to crash the kernel by migrating transparent hugepages.

CVE-2014-9683, Moderate

* A buffer overflow flaw was found in the way the Linux kernel's eCryptfs implementation decoded encrypted file names. A local, unprivileged user could use this flaw to crash the system or, potentially, escalate their privileges on the system.

CVE-2015-3339, Moderate

* A race condition flaw was found between the chown and execve system calls. When changing the owner of a setuid user binary to root, the race condition could momentarily make the binary setuid root. A local, unprivileged user could potentially use this flaw to escalate their privileges on the system.

CVE-2014-3184, Low

* Multiple out-of-bounds write flaws were found in the way the Cherry Cymotion keyboard driver, KYE/Genius device drivers, Logitech device drivers, Monterey Genius KB29E keyboard driver, Petalynx Maxter remote control driver, and Sunplus wireless desktop driver handled HID reports with an invalid report descriptor size. An attacker with physical access to the system could use either of these flaws to write data past an allocated memory buffer.

CVE-2014-4652, Low

* An information leak flaw was found in the way the Linux kernel's Advanced Linux Sound Architecture (ALSA) implementation handled access of the user control's state. A local, privileged user could use this flaw to leak kernel memory to user space.

CVE-2014-8133, Low

* It was found that the espfix functionality could be bypassed by installing a 16-bit RW data segment into GDT instead of LDT (which espfix checks), and using that segment on the stack. A local, unprivileged user could potentially use this flaw to leak kernel stack addresses.

CVE-2014-8709, Low

* An information leak flaw was found in the Linux kernel's IEEE 802.11 wireless networking implementation. When software encryption was used, a remote attacker could use this flaw to leak up to 8 bytes of plaintext.

CVE-2015-0239, Low

* It was found that the Linux kernel KVM subsystem's sysenter instruction emulation was not sufficient. An unprivileged guest user could use this flaw to escalate their privileges by tricking the hypervisor to emulate a SYSENTER instruction in 16-bit mode, if the guest OS did not initialize the SYSENTER model-specific registers (MSRs). Note: Certified guest operating systems for Red Hat Enterprise Linux with KVM do initialize the SYSENTER MSRs and are thus not vulnerable to this issue when running on a KVM hypervisor.

Red Hat would like to thank Andy Lutomirski for reporting the CVE-2014-8133 issue, and Nadav Amit for reporting the CVE-2015-0239 issue.

This update fixes several hundred bugs and adds numerous enhancements. Refer to the Red Hat Enterprise Linux 6.7 Release Notes for information on the most significant of these changes, and the following Knowledgebase article for further information:

https://access.redhat.com/articles/1466073

All kernel users are advised to upgrade to these updated packages, which contain backported patches to correct these issues and add these enhancements. The system must be rebooted for this update to take effect.

7.96. kexec-tools

7.96.1. RHBA-2015:1271 — kexec-tools bug fix and enhancement update

Updated kexec-tools packages that fix several bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

The kexec-tools packages contain the /sbin/kexec binary and utilities that together form the user-space component of the kernel's kexec feature. The /sbin/kexec binary facilitates a new kernel to boot using the kernel's kexec feature either on a normal or a panic reboot. The kexec fastboot mechanism allows booting a Linux kernel from the context of an already running kernel.

Bug Fixes

BZ#1068674

Previously, when the HugePages feature was in use, the makedumpfile utility was unable to exclude these pages based on page type specified with the "-d" option. This led to a much longer dump collection time compared to the same system with no HugePages in use. This bug has been fixed, and the dump collection time is again optimal.

BZ#1208490

When setting up the kdump environment on a system with specific memory hotplug regions and then starting kdump.service, the operating system previously ran out of memory at boot time, and the booting process thus failed. This update adds a parameter to disable memory hotplug for kexec-tools, and the system now boots successfully in the described scenario.

BZ#971017

Prior to this update, /sbin/mkdumprd was not handling the "blacklist [directory]" statement in the /etc/kdump.conf file properly. As a consequence, modules filtered out by "blacklist [directory]" were inserted into the kernel by the initrd block device. The underlying source code has been patched, and mkdumprd now handles the "blacklist [directory]" statement correctly.

BZ#1104837

When cluster ip address was specified as an ip address and not as a resolvable host name, the kdump utility terminated unexpectedly returning error messages. This bug has been fixed, and kdump no longer crashes in the aforementioned situation.

BZ#1131945

Previously, the kdump service was not able to start on iSCSI boot devices during boot because kdump tried to start before the file system was mounted. A patch has been provided to fix this bug, and kdump now starts automatically during boot.

BZ#1132300

When the kdump service was started and no kdump initial ramdisk was present, kdump attempted to rebuild the ramdisk and called the mkdumprd script. As a consequence, two error messages were returned within the "service kdump start" command output. With this update, the user is informed that the FIPS mode will not be enabled while rebuilding the ramdisk, and the error messages are no longer returned.

BZ#1099589

Previously, the mlx4_core driver was excluded from initrd by default as mlx4_core was

consuming too much memory. Nevertheless, the absence of mlx4_core led to problems in the ethernet driver. The fix allows modules that are listed as extra_modules in the /etc/kdump.conf file to load, and the user can now use mlx4_core.

Enhancements

BZ#1195601

The makedumpfile utility now supports the new sadump format that can represent more than 16 TB of physical memory space. This allows users of makedumpfile to read dump files over 16 TB in size, generated by sadump on certain upcoming server models.

BZ#1142666

With this update, the kexec-tools-eppic package has been modified to create a directory for eppic scripts in the /usr/share/ directory. Now, users of kexec-tools-eppic can find some sample eppic scripts for reference though they are contained in the kexec-tools packages.

Users of kexec-tools are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.97. krb5

7.97.1. RHBA-2015:1410 — krb5 bug fix and enhancement update

Updated krb5 packages that fix two bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

Kerberos is a networked authentication system that allows clients and servers to authenticate to each other with the help of a trusted third party, the Kerberos key distribution center.

Bug Fixes

BZ#1075656

Prior to this update, if the Kerberos principal keys were expired, the password change request did not take into account the FAST framework settings for password change requests. Consequently, the pre-auth methods, which require FAST, could not be used for user authentication. This update modifies krb5 to correctly use FAST armor in the password change messages, and the pre-auth methods can be used for user authentication.

BZ#1154130

Previously, after the user set up incremental propagation between a KDC master and slave, an attempt to perform a full synchronization failed with an error message. A patch has been applied to fix this problem, and full synchronization no longer fails after the user sets up incremental propagation between a KDC master and slave.

Enhancement

BZ#1170272

This update adds the LocalAuth plug-in API to krb5. SSSD can leverage LocalAuth to allow seamless authentication of Active Directory (AD) users to Red Hat Enterprise Linux Identity Management (IdM) clients.

Users of krb5 are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

7.98. krb5-auth-dialog

7.98.1. RHBA-2015:0812 — krb5-auth-dialog bug fix update

Updated krb5-auth-dialog packages that fix one bug are now available for Red Hat Enterprise Linux 6.

Kerberos is a networked authentication system which allows clients and servers to authenticate to each other with the help of a trusted third party, the Kerberos key distribution center. The krb5-auth-dialog packages contain a dialog that warns the user when their Kerberos credentials are about to expire and allows them to renew them.

Bug Fix

BZ#848026

Previously, users could experience a disproportionate increase in memory utilization by krb5-auth-dialog after being logged in on VMware virtual machines for longer periods of time. To fix this bug, a patch has been applied. Now, the krb5-auth-dialog memory leak no longer occurs in this situation.

Users of krb5-auth-dialog are advised to upgrade to these updated packages, which fix this bug.

7.99. ksh

7.99.1. RHBA-2015:1450 — ksh bug fix update

Updated ksh packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

KornShell (KSH) is a Unix shell developed by AT&T Bell Laboratories, which is backward-compatible with the Bourne shell (sh) and includes many features of the C shell. The most recent version is KSH-93. KornShell complies with the POSIX.2 standard (IEEE Std 1003.2-1992).

Bug Fixes

BZ#1116072

Prior to this update, the result of a command substitution was lost if a file descriptor used for the substitution was previously explicitly closed. With this update, ksh no longer reuses file descriptors that were closed during the execution of a command substitution. Now, command substitutions work as expected in the described situation.

BZ#1117404

Previously, ksh in some cases terminated unexpectedly when re-setting a trap inside a function. With this update, ksh no longer uses invalid data for trap pointers and does not crash in this situation.

BZ#1160923

After the user changed into a directory that lacked execution permissions, ksh did not recognize that the change did not happen and that the user was instead still operating in the directory from which the user attempted to change. Also, the "pwd" utility incorrectly

displayed the directory into which the user attempted to change instead of the directory in which the user was actually operating. This update modifies ksh to verify whether the directory change was successful. As a result, ksh reports an error if the necessary execution permissions are missing.

BZ#1168611

Previously, ksh sometimes incorrectly initialized a variable holding the path of the working directory. If a program changed the working directory between forking and ksh execution, then ksh could contain an incorrect value in the working directory variable. With this update, initialization of the working directory variable has been corrected, and ksh now contains the correct value in the aforementioned situation.

BZ#1173668

A nested associative array contained an unexpected extra empty value after the array was initialized. This update fixes a bug in the associative array initialization code that was causing this problem. As a result, newly-created nested associative arrays are empty as expected.

BZ#1176670

Previously, ksh terminated unexpectedly after an alarm occurred during a read operation with a modified Internal Field Separator (IFS). The ksh alarm built-in has been modified to preserve the IFS table during execution. As a result, ksh no longer crashes in this situation.

BZ#1188377

When the user set the export attribute to a variable, ksh in certain cases ignored some other variable attributes. For example, when the user set a variable to be both exported and upper-case, ksh did not set the upper-case option correctly. The typeset utility code has been fixed to respect all options that the user sets for a variable. As a result, ksh sets all attributes correctly even if the user sets multiple attributes simultaneously.

BZ#1189294

Previously, after the user unset an associative array, the system did not free the newly-available memory. Consequently, ksh consumed more and more memory over time. The underlying source code has been modified to free the memory after the user unsets an associative array, thus fixing this problem.

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

7.100. lasso

7.100.1. RHBA-2015:1253 — lasso bug fix update

Updated lasso packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The lasso packages provide the Lasso library that implements the Liberty Alliance Single Sign-On standards, including the SAML and SAML2 specifications. It allows handling of the whole life-cycle of SAML-based federations and provides bindings for multiple languages.

Bug Fix

BZ#1160636, BZ#1167796

Users of the lasso packages could previously experience several problems related to Red

Hat Enterprise Linux interoperability with Microsoft Active Directory Federation Services (ADFS). Authentication against ADFS failed when using the mod_auth_mellon module. In addition, in Apache sessions, the limit for the number of elements was insufficient and multi-value variables were not supported. Also, the MellonCond parameter did not work when used together with the MellonSetEnv(NoPrefix) parameter. This update fixes the above described problems with ADFS interoperability.

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

7.101. lftp

7.101.1. RHBA-2015:0793 — lftp bug fix update

Updated lftp packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

LFTP is a file transfer utility for File Transfer Protocol (FTP), Secure Shell File Transfer Protocol (SFTP), Hypertext Transfer Protocol (HTTP), and other commonly used protocols. It uses the readline library for input, and provides support for bookmarks, built-in monitoring, job control, and parallel transfer of multiple files at the same time.

Bug Fixes

BZ#619777

Previously, downloaded files with duplicated names were not renamed even when the "xfer:auto-rename" and "xfer:clobber" options were enabled. To fix this bug, the condition for renaming downloaded files has been modified and they are now renamed as expected.

BZ#674875

Prior to this update, the lftp manual page did not contain information on the "xfer:auto-rename" option. The option has been documented and added to the page, where it is now available to users.

BZ#732863

Due to a bug in error checking code, lftp could fail to connect to a remote host with an IPv6 address if the local host had only IPv4 connectivity, but the remote host domain name was resolved also to IPv6 addresses. With this update, the code has been amended, and the connectivity problems no longer occur in this situation.

BZ#842322

Due to an incorrect evaluation of the length of an uploaded file, the lftp tool became unresponsive after a file transfer in ASCII mode. With this update, the volume of transferred data is recognized correctly and the lftp program no longer hangs in this scenario.

BZ#928307

When running lftp in mirror mode on a website, lftp terminated with an error in cases of HTTP 302 redirection. To fix this bug, lftp has been amended and now successfully proceeds to the new location in such situations.

BZ#1193617

With the "cmd:fail-exit" option enabled, lftp could terminate unexpectedly when any command was executed after the "help" command. With this update, the "help" command has been amended to return correct return code, and lftp no longer exits in this scenario.

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

7.102. libcgroup

7.102.1. RHBA-2015:1263 — libcgroup bug fix update

Updated libcgroup packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The libcgroup packages provide tools and libraries to control and monitor control groups.

Bug Fixes

BZ#1036355

Previously, the cgconfigparser utility wrote the whole multi-line value in a single write() function call, while the 'devices' kernel subsystem expected only one line per write(). Consequently, cgconfigparser did not properly set the multi-line variables. The underlying source code has been fixed, and cgconfigparser now parses all variables as intended.

BZ#1139205

Prior to this update, if '/etc/cgfconfig.conf' or a configuration file in the '/etc/cgconfig.d/' directory contained the cgroup name 'default' that was not enclosed in double quotation marks, backwards compatibility was broken and cgconfigparser failed to parse the file. With this update, 'default' without double quotation marks is again considered a valid cgroup name, and configuration files are now parsed correctly.

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

7.103. libdrm

7.103.1. RHBA-2015:1301 — libdrm, mesa, xorg-x11-drv-ati, and xorg-x11-drv-intel update

Updated libdrm, mesa, xorg-x11-drv-ati, and xorg-x11-drv-intel packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The libdrm packages comprise a runtime library for the Direct Rendering Manager. Mesa provides a 3D graphics API that is compatible with Open Graphics Library (OpenGL) and hardware-accelerated drivers for many popular graphics chips. The xorg-x11-drv-ati packages include a driver for ATI graphics cards for the X.Org implementation of the X Window System. The xorg-x11-drv-intel packages contain an Intel integrated graphics video driver for the X.Org implementation of the X Window System.

Upgrade to an upstream version

The libdrm packages have been upgraded to upstream version 2.4.59, which provides a number of bug fixes and enhancements over the previous version. (BZ#1186821)

* The mesa packages have been upgraded to upstream version 10.4.3, which provides a number of bug fixes and enhancements over the previous version. Among other changes, this version includes support for new Intel 3D graphic chip sets. (BZ#1032663)

* Support for new Intel 3D graphic chip sets has been backported to the xorg-x11-drv-intel packages.

* The xorg-x11-drv-ati packages have been upgraded to upstream version 7.5.99, which contains a number of bug fixes and enhancements over the previous version. Among other changes, this version includes support for new AMD 3D graphic chip sets. (BZ#1176666)

Bug Fixes

BZ#1186821

The libdrm packages have been upgraded to upstream version 2.4.59, which provides a number of bug fixes and enhancements over the previous version.

BZ#1032663

The mesa packages have been upgraded to upstream version 10.4.3, which provides a number of bug fixes and enhancements over the previous version. Among other changes, this version includes support for new Intel 3D graphic chip sets.

BZ#1176666

Support for new Intel 3D graphic chip sets has been backported to the xorg-x11-drv-intel packages.

* The xorg-x11-drv-ati packages have been upgraded to upstream version 7.5.99, which contains a number of bug fixes and enhancements over the previous version. Among other changes, this version includes support for new AMD 3D graphic chip sets.

BZ#1084104

Previously, the radeon driver did not work correctly with the Virtual Network Computing (VNC) module if hardware acceleration was enabled. Consequently, a VNC client connected to a computer set up this way only displayed a blank screen. With this update, this problem has been resolved, and it is now possible to use VNC with the aforementioned setup.

Users of libdrm, mesa, xorg-x11-drv-ati, and xorg-x11-drv-intel are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.104. libguestfs

7.104.1. RHBA-2015:1444 — libguestfs bug fix and enhancement update

Updated libguestfs packages that fix several bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

The libguestfs packages contain a library, which is used for accessing and modifying virtual machine (VM) disk images.

Bug Fixes

BZ#1153855

Using the "virt-sysprep" command to remove a user account from a guest with enabled SELinux did not properly trigger the SELinux relabel process, which caused the guest to be unable to boot. With this update, removing users from such guests properly triggers the relabel. In addition, the virt-sysprep(1) man page now advises to use the "--selinux-relabel" option when cleaning SELinux-enabled guests.

BZ#1100530

The output of the "guestfish -h" command did not include command aliases, which have now been added.

BZ#1056558, BZ#1122557

As a result of the fix for BZ#1056558, it was not possible to use a block device for output when using the virt-sparsify utility. This update re-enables block devices to be used as ouput in virt-sparsify.

BZ#1153846

Using Tab-completion in guestfish on guests with the XFS file system did not correctly append the slash ("/") symbol to directory names. This update adjusts guestfish to properly distinguish files and directories on this file system, and thus fixes the problem.

BZ#1138630

Using the "virt-sysprep" command to remove user accounts did not properly remove the user entries from the /etc/shadow file. With this update, the lens to parse /etc/shadow has been added to the Augeas tool and "virt-sysprep" makes use of it. As a result, removing users from guests using "virt-sysprep" removes also their entries in /etc/shadow.

BZ#1038977

The libguestfs utilities were not able to use disk images on XFS file systems with 4-kilobyte sector size. This update introduces the "cachemode" parameter for the add_drive API, which controls drive caching and has a default value that allows disk images stored on the described file systems to be usable.

BZ#1128942

The libguestfs tools could not use disk images that contained the colon (":") symbol in their path. With this update, path handling in libguestfs and in virt-sparsify has been improved, and such images can now be used as expected.

BZ#1091859

The scrub-file API failed when attempting to handle symbolic links. With this update, scrub-file resolves the file path before handling it further, and as a result, using scrub-file on a symbolic link now properly affects the link's target.

BZ#1159651, BZ#1160203

Due to an incorrect implementation of the libguestfs firstboot scripts runner, the firstboot scripts logged only the last executed script instead of all executed scripts. In addition, firstboot scripts that cause booting to stop, such as a script that reboots the guest, were unintentionally executed on every boot. These problems have now been fixed.

BZ#1074005

In the Java binding, or APIs that return a list of objects different from String caused an ArrayIndexOutOfBoundsException exception to be triggered. The creation of the result list has been fixed, and these APIs now return the expected result.

BZ#1168751

The way in which the lvm-set-filter API handles the lvm.conf file has been rewritten, so that lvm-set-filter is properly able to change the LVM device filter.

Enhancements

BZ#1151901

The output of the "virt-ls --csv --checksum" command now always includes a field for the checksum value, even if the field is empty, like in the case of directories. As a result, the command's output is more easily parseable.

BZ#1164734, BZ#1151739, BZ#1153974, BZ#1100533

Minor fixes and improvements have been done to the help message of the "set-append" command, an error message of the "guestfish umount" command, and to the guestfish(1) and virt-edit(1) man pages.

Users of libguestfs are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.105. libica

7.105.1. RHBA-2015:1283 — libica bug fix and enhancement update

Updated libica packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The libica library contains a set of functions and utilities for accessing the IBM eServer Cryptographic Accelerator (ICA) hardware on IBM System z.

Upgrade to an upstream version

The libica packages have been upgraded to upstream version 2.4.2, which provides a number of bug fixes and enhancements over the previous version, including improved statistics tracking of cryptographic requests issued by libica, increased security of the cryptography library, and enhanced usability that enables better monitoring and debugging of the cryptography stack on IBM System z. (BZ#1148124)

Users of libica are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.106. libpcap

7.106. libpcap

7.106.1. RHBA-2015:1288 — libpcap bug fix update

Updated libpcap packages that fix one bug are now available for Red Hat Enterprise Linux 6.

Libpcap provides a portable framework for low-level network monitoring. Libpcap can provide network statistics collection, security monitoring and network debugging.

Bug Fix

BZ#1025841, BZ#1063328

Previously, running the "tcpdump" command with the filter expression containing the keyword "vlan" produced unexpected output, as the filter generated by the libpcap Berkeley Packet Filter (BPF) compiler did not employ BPF extensions. To fix this bug, libpcap has been amended and now generates filters that use BPF extensions when appropriate. As a result, running "tcpdump" with filters containing "vlan" produces correct results.

Users of libpcap are advised to upgrade to these updated packages, which fix this bug.

7.107. libqb

7.107.1. RHBA-2015:1281 — libqb bug fix and enhancement update

Updated libqb packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The libqb packages provide a library with the primary purpose of providing high performance client server reusable features, such as high performance logging, tracing, inter-process communication, and polling.

Upgrade to an upstream version

The libqb packages have been upgraded to upstream version 0.17.1, which provides a number of bug fixes and enhancements over the previous version. One of the notable changes gives components consuming inter-process communication (IPC) API of libqb more control over IPC buffer sizes. The ability to utilize larger buffer sizes in a consistent way between the IPC client and server allows pacemaker to scale much further in the number of resources the cluster can manage. (BZ#1110042)

Users of libqb are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.108. libreoffice

7.108.1. RHSA-2015:1458 — Moderate: libreoffice security, bug fix, and enhancement update

Updated libreoffice packages that fix one security issue, several bugs, and add various enhancements are now available for Red Hat Enterprise Linux 6.

Red Hat Product Security 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.

LibreOffice is an open source, community-developed office productivity suite. It includes key desktop applications, such as a word processor, a spreadsheet, a presentation manager, a formula editor, and a drawing program. LibreOffice replaces OpenOffice and provides a similar but enhanced and extended office suite.

Security Fix

CVE-2015-1774

A flaw was found in the way the LibreOffice HWP (Hangul Word Processor) file filter processed certain HWP documents. An attacker able to trick a user into opening a specially crafted HWP document could possibly use this flaw to execute arbitrary code with the privileges of the user opening that document.

The libreoffice packages have been upgraded to upstream version 4.2.8.2, which provides a number of bug fixes and enhancements over the previous version. (BZ#1150048)

Bug Fix

BZ#1150048

OpenXML interoperability has been improved.

* This update adds additional statistics functions to the Calc application, thus improving interoperability with Microsoft Excel and its "Analysis ToolPak" add-in.

* Various performance improvements have been implemented in Calc.

* This update adds new import filters for importing files from the Appple Keynote and Abiword applications.

* The export filter for the MathML markup language has been improved.

* This update adds a new start screen that includes thumbnails of recently opened documents.

* A visual clue is now displayed in the Slide Sorter window for slides with transitions or animations.

* This update improves trend lines in charts.

* LibreOffice now supports BCP 47 language tags.

For a complete list of bug fixes and enhancements provided by this rebase, see the libreoffice change log linked from the References section.

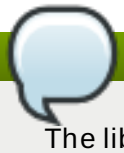
Users of libreoffice are advised to upgrade to these updated packages, which correct these issues and add these enhancements.

7.109. librtas

7.109.1. RHBA-2015:1304 — librtas bug fix and enhancement update

Updated librtas packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The librtas packages contain a set of libraries that allow access to the Run-Time Abstraction Services (RTAS) on 64-bit PowerPC architectures. The librtasevent library contains definitions and routines for analyzing RTAS events.



Upgrade to an upstream version

The librtas packages have been upgraded to upstream version 1.3.13, which provides a number of bug fixes and enhancements over the previous version. (BZ#1148742)

Users of librtas are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.110. libsemanage

7.110.1. RHBA-2015:1403 — libsemanage bug fix update

Updated libsemanage packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The libsemanage library provides an API for the manipulation of SELinux binary policies. It is used by the checkpolicy compiler and similar tools, as well as by programs such as load_policy, which must perform specific transformations on binary policie, such as customizing policy boolean settings.

Bug Fixes

BZ#591451

The libsemanage test suite previously failed when attempting to test the libsemanage library. With this update, an error in the underlying code has been corrected, which allows the libsemanage test suite to work as expected.

BZ#872700

Prior to this update, the semodule command failed with an error message when attempting to enable an already enabled module, or disable an already disabled module. This update adjusts the behavior of the command to succeed and not to produce error messages in the described scenarios.

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

7.111. libvirt

7.111.1. RHBA-2015:1252 — libvirt bug fix update

Updated libvirt packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The libvirt library is a C API for managing and interacting with the virtualization capabilities of Linux and other operating systems.

Bug Fixes

BZ#1198096

Previously, when the default CPU mask was specified while using Non-Uniform Memory Access (NUMA) pinning, virtual CPUs (vCPUs) could not be pinned to physical CPUs that were not contained in the default node mask. With this update, the control groups (cgroups) code correctly attaches only vCPU threads instead of the entire domain group, and using NUMA pinning with the default cpuset subsystem now works as expected.

BZ#1186142

The interface configuration of any libvirt domain which was of type='network' and referenced an "unmanaged" libvirt network had incorrect XML data for the interface transmitted during a migration, containing the "status" of the interface instead of the name of the network to use ("configuration"). As a consequence, the migration destination tried to set up the domain network interface using the status information from the source of the migration, and the migration thus failed. With this update, libvirt sends the configuration data for each device during migration rather than the status data, and the migration of a domain using interfaces of type='network' now succeeds.

BZ#1149667

In Red Hat Enterprise Linux 6.6, support was added for libvirt to report whether QEMU is capable of creating snapshots. However, libvirt did not probe for the snapshot capability properly. As a consequence, the snapshot capability of KVM Guest Image in VDSM was reported as unavailable even when it was available, and creating a disk snapshot in some cases failed. With this update, libvirt no longer reports QEMU snapshot capability, and therefore does not cause the described problem.

BZ#1138523

Previously, using the "virsh pool-refresh" command, or restarting or refreshing the libvirtd service after renaming a virtual storage volume in some cases caused the "virsh vol-list" to display an incorrect name for the renamed storage volume. This update adds a check for the resulting name, which returns an error if the storage volume name is incorrect.

BZ#1158036

Prior to this update, when using the "virsh save" command to save a domain to an NFS client with the "root squash" access rights reduction while running the libvirtd service with a non-default owner:group configuration, saving the NFS client failed with a "Transport endpoint is not connected" error message. This update ensures that the chmod operation during the saving process correctly specifies the non-default owner:group configuration, and using "virsh save" in the described scenario works as expected.

BZ#1113474

A virtual function (VF) could not be used in the macvtap-passthrough network if it was previously used in the hostdev network. With this update, libvirt ensures that the VF's MAC address is properly adjusted for the macvtap-passthrough network, which allows the VF to be used properly in the described scenario.

Users of libvirt are advised to upgrade to these updated packages, which fix these bugs. After installing the updated packages, libvirtd will be restarted automatically.

7.112. libxcb

7.112.1. RHBA-2015:1358 — libxcb and libX11 bug fix update

Updated libxcb and libX11 packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The libxcb packages provide the X protocol C-language Binding (XCB) library. XCB is a replacement for Xlib featuring a small footprint, latency hiding, direct access to the protocol, improved threading support, and extensibility. The libX11 packages contain the core X11 protocol client library.

Bug Fixes

BZ#667789

Previously, the "mute microphone" key in some cases did not work when using Red Hat Enterprise Linux 6. With this update, libX11 properly resolves the key symbol assigned to the "mute microphone" key by the xkeyboard-config keyboard layout files, and the "mute microphone" key now works as expected.

BZ#1206240, BZ#1046410, BZ#1164296

On 32-bit architectures, an X11 protocol client was under certain circumstances disconnected after processing a large number of X11 requests. With this update, the libxcb library exposes the request sequence number as a 64-bit integer so that libX11 can make use of 64-bit sequence number even on 32-bit systems. As a result, the described failure of the X11 client no longer occurs.

Users of libxcb and libX11 are advised to upgrade to these updated packages, which fix these bugs.

7.113. libxml2

7.113.1. RHSA-2015:1419 — Low: libxml2 security and bug fix update

Updated libxml2 packages that fix one security issue and one bug are now available for Red Hat Enterprise Linux 6.

Red Hat Product Security 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 libxml2 library is a development toolbox providing the implementation of various XML standards.

Security Fix

CVE-2015-1819

A denial of service flaw was found in the way the libxml2 library parsed certain XML files. An attacker could provide a specially crafted XML file that, when parsed by an application using libxml2, could cause that application to use an excessive amount of memory.

This issue was discovered by Florian Weimer of Red Hat Product Security.

Users of libxml2 are advised to upgrade to these updated packages, which contain backported patches to correct these issues. The desktop must be restarted (log out, then log back in) for this update to take effect.

7.114. linuxptp

7.114.1. RHBA-2015:1321 — linuxptp bug fix and enhancement update

Updated linuxptp packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The linuxptp packages provide Precision Time Protocol (PTP) implementation for Linux according to IEEE standard 1588 for Linux. The dual design goals are to provide a robust implementation of the standard and to use the most relevant and modern Application Programming Interfaces (API) offered by the Linux kernel.

Upgrade to an upstream version

The linuxptp packages have been upgraded to upstream version 1.5, which provides a number of bug fixes and enhancements over the previous version. (BZ#1190222)

Enhancement

BZ#1085584

This update adds support for failover between Precision Time Protocol (PTP) domains or Network Time Protocol (NTP) sources. The system is now able to fall back to an alternate time source if PTP becomes unavailable, or maintain PTP synchronization in the event of Network Interface Controller (NIC) failure by using another NIC in the system.

Users of linuxptp are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.115. logrotate

7.115.1. RHBA-2015:1293 — logrotate bug fix and enhancement update

Updated logrotate packages that fix several bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

The logrotate utility simplifies the administration of multiple log files, allowing the automatic rotation, compression, removal, and mailing of log files.

Bug Fixes

BZ#625034

When the logrotate utility attempted to write its status file while insufficient disk space was available, logrotate wrote only part of the status file and stopped. When the disk space became free again, and log rotate attempted to read its records, logrotate terminated unexpectedly. This bug has been fixed, and logrotate no longer crashes in the aforementioned scenario.

BZ#722209

Previously, the daily cronjob of logrotate redirected all error messages to the /dev/null device file, thus suppressing all the relevant information for troubleshooting. With this update, all error messages containing detailed error reports are mailed to the root user. In addition, the /etc/cron.daily/logrotate file has been marked as a configuration file in RPM.

BZ#1012485

Previously, the /etc/cron.daily/logrotate file had incorrect permissions set. This update

changes the permissions to 0700, and /etc/cron.daily/logrotate now conforms to Red Hat security policy GEN003080.

BZ#1117189

The logrotate utility incorrectly deleted data files alphabetically instead of based on their age when the when the "-%d-%m-%Y" date format was used. This update sorts files returned by the glob() function according to the date extension. As a result, when the aforementioned date format is used, the oldest log is now removed as expected.

Enhancements

BZ#1125769

The logrotate "olddir" directive now automatically creates a directory if it is not already present.

BZ#1047899

This update adds logrotate features for "size" directive parsing and "maxsize" directive.

Users of logrotate are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.116. lsof

7.116.1. RHBA-2015:1246 — lsof bug fix update

Updated lsof packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The lsof (LiSt Open Files) package provides a utility to list information about files that are open by the processes running on Linux and UNIX systems.

Bug Fixes

BZ#772991

Prior to this update, the lsof utility could, under certain circumstances, report incorrect server locations of mounted folders if multiple Network File System (NFS) shares from one host were mounted. This update allows multiple NFS clients to share superblocks. Now, lsof reports the correct server locations of mounted folders.

BZ#668099

Previously, lsof did not recognize Stream Control Transmission Protocol (SCTP) associations and consequently printed "can't identify protocol" at the end of the line describing a process using this type of association. With this update, support for SCTP has been added, and as a result, lsof correctly identifies SCTP associations in its output.

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

7.117. lsscsi

7.117.1. RHBA-2015:0798 — lsscsi bug fix update

Updated lsscsi packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The lsscsi utility uses information provided by the sysfs pseudo file system in Linux kernel 2.6 and later series to list small computer system interface (SCSI) devices or all SCSI hosts attached to the system. Options can be used to control the amount and form of information provided for each device.

Bug Fix

BZ#1009883

The lsscsi package has been updated to properly detect and decode the SCSI "protection_type" and "integrity" flags. Previously, the lsscsi package tried to read the "protection_type" and "integrity" flags from a location in the sysfs file system where they were not expected to be found. With this update, lsscsi now uses the proper file locations to identify these flags.

Users of lsscsi are advised to upgrade to these updated packages, which fix this bug.

7.118. luci

7.118.1. RHBA-2015:1454 — luci bug fix and enhancement update

Updated luci packages that fix several bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

The luci package provides a web-based high-availability cluster configuration application built on the TurboGears 2 framework.

Bug Fixes

BZ#1136456

When editing the cluster configuration, if an error occurred while attempting to set the new configuration on one or more nodes, luci still attempted to activate the new configuration version. As a consequence, the cluster could fall out of sync. With this update, luci no longer activates a new cluster configuration in the described situation.

BZ#1010400

A new attribute, "cmd_prompt" has been added to the fence_apc fence agent. Consequently, users could not view and change this new attribute. The fence_apc form has been updated to include support for viewing and setting "cmd_prompt.

BZ#1111249

The "stop" action semantics differ from the "disable" action semantics in the rgmanager utility. Previously, after clicking the "stop" button in the GUI, luci always issued a command that caused the "disable" action to be issued in rgmanager. As a consequence, luci could not issue a command that would cause the rgmanager "stop" action to be issued for a service. This update adds a "stop" action in addition to the "disable" action that is accessible only in expert mode.

BZ#886526

After selecting "add resource" for a service group, a cancel button was missing from the dialog, which created a dead-end in the GUI. As a consequence, users had to reload the page if they clicked the button accidentally or wanted to change their choice after clicking it. This update adds a cancel button to the "add resource" dialog for service groups.

BZ#1100831

Previously, luci did not allow VM resources to have children resources, and after adding a VM to a service group, the "add resource" button was removed so that no further resources could be added. However, the GUI could handle configurations that contained resources with children. As a consequence, even though luci supported the aforementioned configurations, the "add resource" button was removed after adding a VM resource. With this update, the "add resource" button is no longer removed when adding a VM resource to a service group.

BZ#917781

The luci tool allowed setting the "shutdown_wait" attribute for postgres-8 resources, but the resource agent ignored the attribute. Consequently, it was not clear that "shutdown_wait" no longer had any effect. This update adds a text for clusters running Red Hat Enterprise Linux 6.2 and later to indicate that the "shutdown_wait" parameter is ignored.

BZ#1204910

Starting with Red Hat Enterprise Linux 6.7, fence_virt is fully supported. Previously, fence_virt was included as a Technology Preview, which was indicated by a label in the GUI. Also, certain labels and text regarding fence_xvm and fence_virt were inconsistent. With this update, the GUI text reflects the current support status for fence_virt and the the text is consistent.

BZ#1112297

When making changes to certain resources, service groups, and fence agents while not in expert mode, attributes that could be set with luci only in expert mode could be lost. As a consequence, some configuration parameters could be erroneously removed. With this update, luci no longer removes expert-mode-only attributes.

Enhancements

BZ#1210683

Support for configuring the fence_emerson and fence_mpath fence devices has been added to luci.

BZ#919223

With this update, users can collapse and expand parts of service groups when viewing or editing service groups in luci, which improves the usability, as the configuration screen could previously become too cluttered.

Users of luci are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.119. lvm2

7.119.1. RHBA-2015:1411 — lvm2 bug fix and enhancement update

Updated lvm2 packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The lvm2 packages include complete support for handling read and write operations on physical volumes (PVs), creating volume groups (VGs) from one or more PVs, and creating one or more logical volumes (LVs) in VGs.

Two enhancements are described in the Red Hat Enterprise Linux 6.7 Release Notes, linked from the References section:

Bug Fixes

BZ#853259

This update enhances selection support in the Logical Volume Manager (LVM)

BZ#1021051

The "lvchange -p" command can change in-kernel permissions on a logical volume (LV)

BZ#736027

Volume groups (VGs) built from a high number of physical volumes (PVs) can experience significant lags. Enabling the lvmetad service reduces the operation time even on systems where the VG has metadata on all PVs.

BZ#1021728

The lvremove utility failed to remove damaged thin pools that were not repaired. The double "--force --force" option can now remove such pool volumes.

BZ#1130245

When the lvmetad service was used with "global/use_lvmetad=1" set, LVM leaked open sockets, and lvmetad kept threads for existing sockets. Now, LVM no longer leaks open lvmetad sockets, and lvmetad frees unused threads.

BZ#1132211

Activating a thin pool failed under certain circumstances. The lvm2 utility now properly rounds to 64 kB thin pool chunk size, thus fixing this bug.

BZ#1133079

The lvconvert utility displayed internal error messages under certain circumstances. Now, lvconvert verifies if the "--originname" value differs from the "--thinpool" value before the conversion begins. The messages are no longer displayed.

BZ#1133093

The user could not use the lvconvert utility to repair or split mirrors from cache data and cache metadata volumes due to strict checks for LV names. The checks have been relaxed, and lvconvert can be successfully used for these operations.

BZ#1136925

The lvm2 utility previously in some cases attempted to access incorrect devices for locking. Now, lvm2 uses the expected LV lock for snapshot volumes, thus fixing this bug.

BZ#1140128

When the volume_list parameter was set to forbid activating volumes during thin pool creation on error code path, some volumes could remain active in the device mapper table without the proper lock being held. All such volumes are now correctly deactivated before lvm2 exits.

BZ#1141386

Changing the VG clustering attribute could malfunction when clustered locking was selected. The code now correctly checks and propagates locks even for non-clustered VGs in this situation. The bug no longer occurs.

BZ#1143747

It is no longer possible to set the "--minor" and "--major" options for thin pool volumes with the lvm2 utility. If the user attempts to set them, lvm2 correctly informs the user they are not supported.

BZ#1171805, BZ#1205503

The vgimportclone script did sometimes not work as expected and in some cases also failed to rename and import duplicated VGs. The script now properly handles when the "filter" setting is missing from the lvm.conf file, and its code has been made more robust, thus fixing these bugs.

BZ#1184353

The "--clear-needs-check-flag" option was missing from the default value for the thin_check_options option in the "global" section of the lvm.conf file after installing lvm2. Now, "--clear-needs-check-flag" is set by default after installation.

BZ#1196767

The pvs utility did not list all PVs when reporting only label fields for given PVs if "obtain_device_list_from_udev=0" was set in lvm.conf. Now, LVM2 generates correct content for the persistent cache, thus fixing this bug.

Enhancements

BZ#1202916

With this update, LVM cache is fully supported. Users can now create LVs with a small fast device that serves as a cache to larger and slower devices. For information on creating cache LVs, see the lvmcache(7) man page.

BZ#1211645

This update adds the "--enable-halvm", "--disable-halvm", "--mirrorservice", and "--startstopservices" options to the lvmconf script. For more information, see the lvmconf(8) man page.

Users of lvm2 are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.120. mailman

7.120.1. RHSA-2015:1417 — Moderate: mailman security and bug fix update

Updated mailman packages that fix two security issues and several bugs are now available for Red Hat Enterprise Linux 6.

Red Hat Product Security 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 e-mail discussion lists.

Security Fixes

CVE-2015-2775

It was found that mailman did not sanitize the list name before passing it to certain MTAs. A local attacker could use this flaw to execute arbitrary code as the user running mailman.

CVE-2002-0389

It was found that mailman stored private email messages in a world-readable directory. A local user could use this flaw to read private mailing list archives.

Bug Fixes

BZ#1095359

Previously, it was impossible to configure Mailman in a way that Domain-based Message Authentication, Reporting & Conformance (DMARC) would recognize Sender alignment for Domain Key Identified Mail (DKIM) signatures. Consequently, Mailman list subscribers that belonged to a mail server with a "reject" policy for DMARC, such as yahoo.com or AOL.com, were unable to receive Mailman forwarded messages from senders residing in any domain that provided DKIM signatures. With this update, domains with a "reject" DMARC policy are recognized correctly, and Mailman list administrators are able to configure the way these messages are handled. As a result, after a proper configuration, subscribers now correctly receive Mailman forwarded messages in this scenario.

BZ#1056366

Mailman used a console encoding when generating a subject for a "welcome email" when new mailing lists were created by the "newlist" command. Consequently, when the console encoding did not match the encoding used by Mailman for that particular language, characters in the "welcome email" could be displayed incorrectly. Mailman has been fixed to use the correct encoding, and characters in the "welcome email" are now displayed properly.

BZ#1008139

The "rmlist" command used a hardcoded path to list data based on the VAR_PREFIX configuration variable. As a consequence, when the list was created outside of VAR_PREFIX, it was impossible to remove it using the "rmlist" command. With this update, the "rmlist" command uses the correct LIST_DATA_DIR value instead of VAR_PREFIX, and it is now possible to remove the list in described situation.

BZ#765807

Due to an incompatibility between Python and Mailman in Red Hat Enterprise Linux 6, when moderators were approving a moderated message to a mailing list and checked the "Preserve messages for the site administrator" checkbox, Mailman failed to approve the message and returned an error. This incompatibility has been fixed, and Mailman now approves messages as expected in this scenario.

BZ#745409

When Mailman was set to not archive a list but the archive was not set to private, attachments sent to that list were placed in a public archive. Consequently, users of Mailman web interface could list private attachments because httpd configuration of public archive directory allows listing all files in the archive directory. The httpd configuration of Mailman has been fixed to not allow listing of private archive directory, and users of Mailman web interface are no longer able to list private attachments.

Users of mailman are advised to upgrade to these updated packages, which contain backported patches to correct these issues.

7.121. man-pages-fr

7.121.1. RHBA-2015:0667 — man-pages-fr bug fix update

An updated man-pages-fr package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The man-pages-fr package contains a collection of manual pages translated into French.

Bug Fix

BZ#1135541

The French version of the "du" man page does not contain an up-to-date list of "du" options and their descriptions. Because the man page is no longer maintained, this update adds a message at the top of the page stating that the documentation is outdated, and that users can find the latest version in the English man page.

Users of man-pages-fr are advised to upgrade to this updated package, which fixes this bug.

7.122. man-pages-ja

7.122.1. RHBA-2015:0665 — man-pages-ja bug fix update

An updated man-pages-ja package that fixes several bugs is now available for Red Hat Enterprise Linux 6.

The man-pages-ja package contains manual pages in Japanese.

Bug Fixes

BZ#1157413

The date(1) man page did not mention options "%n" and "%N". which print a newline character and the number of nanoseconds respectively. This update adds these options and their descriptions to the man page.

BZ#1173391

The nfs(5) man page did not include the remark on the obsolescence of the "intr" and "nointr" options which is part of the English man page. With this update, the Japanese man page now includes this remark.

BZ#1174088

Previously, incorrect location of the output file for an internal state dump, /tmp/xinetd.dump, was specified in the xinetd(8) man page, in the section describing the action that xinetd performs when it receives the SIGUSR1 signal. The correct location is /var/run/xinetd.dump, and it is now written in the man page.

BZ#1140481

The description of the "EINVAL" error code in the shmop(2) man page was accidentally placed on the line describing the preceding error code, "EIDRM". This update moves the description of "EINVAL" into a separate paragraph.

Users of man-pages-ja are advised to upgrade to this updated package, which fixes these bugs.

7.123. man-pages-overrides

7.123.1. RHBA-2015:1295 — man-pages-overrides bug fix update

An updated man-pages-overrides package that fixes several bugs is now available for Red Hat Enterprise Linux 6.

The man-pages-overrides package provides a collection of manual (man) pages to complement other packages or update those contained therein.

Bug Fixes

BZ#1205351

Previously, the eventfd(2) manual page did not describe the EFD_SEMAPHORE flag, although the kernel supported this feature. This update adds the missing details about EFD_SEMAPHORE to eventfd(2).

BZ#1207200

The yum-security(8) manual page contained insufficient information about package selection mechanism of the "update-minimum" command with the "--advisory" option. This update adds a more detailed explanation of this process, including an example syntax.

BZ#1140473

Previously, the description of the %util field in the iostat(1) and sar(1) manual pages was incorrect. The description of %util has been fixed, and documentation of the iostat and sar commands is now correct.

BZ#1205377

The pthread_kill(3) manual page contained incorrect information about a possibility to use the pthread_kill() function to check for the existence of a thread ID. Consequently, following this instruction led to a segmentation fault in case of a non-existent thread ID. The misleading piece of information has been removed and pthread_kill(3) now includes more details about handling of non-existent thread IDs.

BZ#1159335

Previously, the statfs struct section in the statfs(2) manual page did not mention the "f_flags" and "f_spare" fields. This update adds the missing fields to statfs(2).

BZ#1121700

The reposync(1) manual page did not contain descriptions of the "e", "d", "m", and "norepopath" options. With this update, reposync(1) provides the complete list of options and their descriptions.

BZ#1159842

Prior to this update, certain manual pages in Russian language were incorrectly encoded. As a consequence, users were unable to read such man pages. This bug has been fixed, and man pages are displayed in the correct encoding.

Users of man-pages-overrides are advised to upgrade to this updated package, which fixes these bugs.

7.124. mcelog

7.124.1. RHBA-2015:1303 — mcelog bug fix and enhancement update

Updated mcelog packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The mcelog packages contain a daemon that collects and decodes Machine Check Exception (MCE) data on AMD64 and Intel 64 machines.

Upgrade to an upstream version

The mcelog packages have been upgraded to upstream version 109, which provides a number of bug fixes and enhancements over the previous version. Notably, mcelog now supports Intel Core i7 CPU architectures. (BZ#1145371)

Users of mcelog are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.125. mdadm

7.125.1. RHBA-2015:1255 — mdadm bug fix and enhancement update

Updated mdadm packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The mdadm packages contain a utility for creating, managing, and monitoring Linux multiple disk (MD) devices.

Bug Fixes

BZ#1146536

Previously, installing the mdadm packages also installed a redundant udev rule file. With this update, the spec file of the mdadm packages has been adjusted to prevent the redundant rule file from being installed.

BZ#1159399

Prior to this update, when the "AUTO" keyword was configured in the mdadm.conf file, the mdadm utility did not behave accordingly. The parsing of "AUTO" has been corrected, and mdadm now respects this keyword as expected.

BZ#1146994

Prior to this update, when running an Internal Matrix Storage Manager (IMSM) volume as a non-root user, a race condition in some cases occurred that prevented the assembly of the volume. With this update, the mdadm packages have been fixed and this race condition no longer occurs, allowing the array to be assembled as expected.

BZ#1211564

Previously, mdadm was unintentionally capable of creating more Internal Matrix Storage Manager (IMSM) raid volumes than was allowed by the "Max volumes" option in mdadm configuration. This update corrects the bug, and attempting to create a more IMSM raid volumes than set by "Max volumes" now generates an error and does not create the raid volumes.

Enhancement

BZ#1211500

Internal Matrix Storage Manager (IMSM) now supports SATA and Non-volatile memory Express (NVMe) spanning.

Users of mdadm are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.126. mercurial

7.126.1. RHBA-2015:1436 — mercurial bug fix update

Updated mercurial packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

Mercurial is a lightweight source control management system designed for managing large distributed projects.

Bug Fixes

BZ#784079

Previously, the "hg view" command failed with the "Permission denied" error message. This update adds the required execute permission to the hgk utility. As a result, running "hg view" works as expected.

BZ#928301

Running an SSL-encrypted "hg serve" command could previously cause the server to rise an exception and tracebacks on every SSL connection attempt. As a consequence, "hg serve" failed in this situation even though it worked as expected without SSL. A patch has been applied to fix this bug. As a result, running SSL-encrypted "hg serve" works, and the command displays the expected output.

BZ#1006457

Prior to this update, running the "hg copy -A" command did not add broken symbolic links to a repository. The underlying source code has been modified to use the os.patch.lexists() method. As a result, "hg copy -A" adds the broken symbolic links as expected.

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

7.127. mgetty

7.127.1. RHBA-2015:0711 — mgetty bug fix update

Updated mgetty packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The mgetty packages contain a modem getty utility that allows logins over a serial line, for example using a modem. If you are using a Class 2 or Class 2.0 modem, mgetty can receive faxes. The mgetty-sendfax package is required to send faxes.

Bug Fix

BZ#729003

Missing files with debug information have been added to the mgetty-debuginfo packages for seven binary files shipped in the mgetty package.

Users of mgetty are advised to upgrade to these updated packages, which fix this bug.

7.128. microcode_ctl

7.128.1. RHEA-2015:1291 — microcode_ctl enhancement update

Updated microcode_ctl packages that add one enhancement are now available for Red Hat Enterprise Linux 6.

The microcode_ctl packages provide microcode updates for Intel and AMD processors.

Enhancement

BZ#1123992

An updated CPU Microcode data file is now available to be used by the Linux kernel to correct behavior in Intel processors on boot.

Users of microcode_ctl are advised to upgrade to these updated packages, which add this enhancement. Note: a system reboot is necessary for this update to take effect.

7.129. mlocate

7.129.1. RHBA-2015:0676 — mlocate bug fix update

Updated mlocate packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The mlocate packages provide a locate/updatedb implementation, and keep a database of all existing files. The database allows files to be looked up by names.

Bug Fixes

BZ#1012534

Prior to this update, the cron script which is included in the mlocate packages had permissions which were too loose. Consequently, mlocate did not comply with the Operating System Security Requirements Guide. This update changes the permissions of the cron script to 0700, as required by the guide.

BZ#1023779

The updatedb utility automatically excludes file systems which are marked as "nodev" in the /proc/filesystems file. The ZFS file system is also marked this way despite the fact it actually stores data on a physical device. As a consequence, ZFS volumes were not previously indexed. This update adds an exception for ZFS, which allows updatedb to index files stored on this file system and the locate utility to find such files.

BZ#1182304

Previously, the /var/lib/mlocate/mlocate.db database file was declared in the mlocate package metadata as belonging to the "root" user and group, and having the "644" permissions. However, in reality, the file belonged to the "slocate" group and had the "640" permissions. This discrepancy caused problems reported by OpenSCAP compliance checking tools. With this update, the database file is declared correctly in the metadata, which allows the package in an unaltered state to pass OpenSCAP compliance checks.

BZ#1168301

The updatedb utility did not exclude GPFS cluster file systems, which can hold billions of files. As a consequence, updatedb caused very high I/O load on systems using GPFS. With this update, GPFS volumes are skipped by updatedb. As a result, files stored on this file system are no longer indexed, and running updatedb on systems with GPFS volumes does not cause too high I/O load.

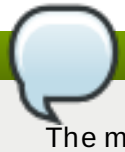
Users of mlocate are advised to upgrade to these updated packages, which fix these bugs.

7.130. mod_nss

7.130.1. RHBA-2015:1284 — mod_nss bug fix and enhancement update

Updated mod_nss packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

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.



Upgrade to an upstream version

The mod_nss packages have been upgraded to upstream version 1.0.10, which provides a number of bug fixes and enhancements over the previous version. Most notably, this update adds support for TLS version 1.2 to mod_nss. (BZ#1166316)

Users of mod_nss are advised to upgrade to these updated packages, which fix these bugs and add these enhancements. The httpd service must be restarted for this update to take effect.

7.131. module-init-tools

7.131.1. RHBA-2015:1289 — module-init-tools bug fix update

Updated module-init-tools packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The module-init-tools packages include various programs needed for automatic loading and unloading of modules under 2.6 kernels, as well as other module management programs. Device drivers and file systems are two examples of loaded and unloaded modules.

Bug Fix

BZ#1101045

On systems where the bridge module was not loaded, the "sysctl -p" command previously returned an error. This update moves several net.bridge.bridge-nf-call* parameters from the /etc/sysctl.conf file to the /etc/modprobe.d/dist.conf file, so that they take effect only when the bridge module is loaded, instead of being a part of the system startup. As a result, the described problem no longer occurs.

Users of module-init-tools are advised to upgrade to these updated packages, which fix this bug.

7.132. nc

7.132.1. RHEA-2014:1968 — nc bug fix update

Updated nc packages that add two enhancements are now available for Red Hat Enterprise Linux 6.

The nc packages contain the nc (or netcat) utility for reading and writing data across network connections, by using the TCP and UDP protocols. Also, netcat can be used as a feature-rich network debugging and exploration tool, as netcat can create many different connections and has numerous built-in capabilities.

Enhancements

BZ#1000773

With this update, the netcat utility can handle HTTP/1.1 proxy responses, which certain proxies send in response to HTTP/1.0 requests.

BZ#1064755

This update improves the phrasing of comments that contained profanities in certain sections in scripts provided by the netcat utility.

Users of nc are advised to upgrade to these updated packages, which add these enhancements.

7.133. ncurses

7.133.1. RHBA-2015:0687 — ncurses bug fix update

Updated ncurses packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The ncurses (new curses) library routines are a terminal-independent method of updating character screens with reasonable optimization. The ncurses packages contain support utilities including a terminfo compiler tic, a decompiler infocmp, clear, tput, tset, and a termcap conversion tool captoinfo.

Bug Fix

BZ#1025744

Prior to this update, compilation of applications that use pkg-config and static linking could fail, as the ncurses.pc files did not include the "-ltinfo" option for static linking with ncurses. To fix this bug, the "-ltinfo" option has been included in the pkg-config files and applications now compile successfully.

Users of ncurses are advised to upgrade to these updated packages, which fix this bug.

7.134. net-snmp

7.134.1. RHSA-2015:1385 — Moderate: net-snmp security and bug fix update

Updated net-snmp packages that fix one security issue and several bugs are now available for Red Hat Enterprise Linux 6.

Red Hat Product Security 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 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.

Security Fix

CVE-2014-3565

A denial of service flaw was found in the way snmptrapd handled certain SNMP traps when started with the "-OQ" option. If an attacker sent an SNMP trap containing a variable with a NULL type where an integer variable type was expected, it would cause snmptrapd to crash.

Bug Fixes

BZ#1134335

The HOST-RESOURCES-MIB::hrSystemProcesses object was not implemented because parts of the HOST-RESOURCES-MIB module were rewritten in an earlier version of net-snmp. Consequently, HOST-RESOURCES-MIB::hrSystemProcesses did not provide information on the number of currently loaded or running processes. With this update, HOST-RESOURCES-MIB::hrSystemProcesses has been implemented, and the net-snmp daemon reports as expected.

BZ#789500

The Net-SNMP agent daemon, snmpd, reloaded the system ARP table every 60 seconds. As a consequence, snmpd could cause a short CPU usage spike on busy systems with a large APR table. With this update, snmpd does not reload the full ARP table periodically, but monitors the table changes using a netlink socket.

BZ#1050970

Previously, snmpd used an invalid pointer to the current time when periodically checking certain conditions specified by the "monitor" option in the /etc/snmpd/snmpd.conf file. Consequently, snmpd terminated unexpectedly on start with a segmentation fault if a certain entry with the "monitor" option was used. Now, snmpd initializes the correct pointer to the current time, and snmpd no longer crashes on start.

BZ#1195547

Previously, snmpd expected 8-bit network interface indices when processing HOST-RESOURCES-MIB::hrDeviceTable. If an interface index of a local network interface was larger than 30,000 items, snmpd could terminate unexpectedly due to accessing invalid memory. Now, processing of all network sizes is enabled, and snmpd no longer crashes in the described situation.

BZ#1146948

The snmpdtrapd service incorrectly checked for errors when forwarding a trap with a RequestID value of 0, and logged "Forward failed" even though the trap was successfully forwarded. This update fixes snmptrapd checks and the aforementioned message is now logged only when appropriate.

BZ#1125793

Previously, snmpd ignored the value of the "storageUseNFS" option in the /etc/snmpd/snmpd.conf file. As a consequence, NFS drivers were shown as "Network Disks", even though "storageUseNFS" was set to "2" to report them as "Fixed Disks" in HOST-RESOURCES-MIB::hrStorageTable. With this update, snmpd takes the "storageUseNFS" option value into account, and "Fixed Disks" NFS drives are reported correctly.

BZ#1100099

Previously, the Net-SNMP python binding used an incorrect size (8 bytes instead of 4) for variables of IPADDRESS type. Consequently, applications that were using Net-SNMP Python bindings could send malformed SNMP messages. With this update, the bindings now use 4 bytes for variables with IPADRESS type, and only valid SNMP messages are sent.

BZ#1104293

Previously, the snmpd service did not cut values in HOST-RESOURCES-MIB::hrStorageTable to signed 32-bit integers, as required by SNMP standards, and provided the values as unsigned integers. As a consequence, the HOST-RESOURCES-MIB::hrStorageTable implementation did not conform to RFC 2790. The values are now cut to 32-bit signed integers, and snmpd is therefore standard compliant.

Users of net-snmp are advised to upgrade to these updated packages, which contain backported patches to correct these issues.

7.135. netcf

7.135.1. RHBA-2015:1307 — netcf bug fix update

Updated netcf packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The netcf packages contain a library for modifying the network configuration of a system. Network configuration is expressed in a platform-independent XML format, which netcf translates into changes to the system's "native" network configuration files.

Bug Fixes

BZ#1113978

Previously, when the XML configuration for an interface enabled dynamic host

configuration protocol (DHCP) for IPv6, the netcf library erroneously set the variable named "DHCPV6" in the ifcfg configuration file instead of "DHCPV6C". The underlying source code has been patched, and netcf now passes the correct "DHCPV6C" option to ifcfg.

BZ#1116314

Prior to this update, when requested to configure an interface with an IPv4 netmask of 255.255.255.255, the netcf library logged an error as the interface configuration was rejected. This update fixes the netmask for the 32-bit interface prefix, and netcf now configures IPv4 interfaces successfully.

BZ#1208897

Due to a parsing error, the ifcfg files with comments starting anywhere beyond column 1 or multiple variables on a single line caused the netcf library to generate errors when attempting to list host interfaces. The parsing error has been fixed, and any tool using netcf now lists active interfaces as expected.

BZ#1208894

When multiple static IPv6 addresses were specified in an interface configuration, an extra set of quotes appeared in the IPV6ADDR_SECONDARIES entry in the generated configuration file. This update removes extraneous single quotes from IPV6ADDR_SECONDARIES, thus fixing this bug.

BZ#1165966

Due to a denial of a service flaw in the netcf library, a specially crafted interface name previously caused applications using netcf, such as the libvirt daemon, to terminate unexpectedly. An upstream patch has been applied to fix this bug, and applications using netcf no longer crash in the aforementioned situation.

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

7.136. nfs-utils

7.136.1. RHBA-2015:1342 — nfs-utils bug fix and enhancement update

Updated nfs-utils packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The nfs-utils packages provide a daemon for the kernel Network File System (NFS) server and related tools, which provides better performance than the traditional Linux NFS server used by most users. These packages also contain the mount.nfs, umount.nfs, and showmount programs.

Bug Fixes

BZ#1007281

Previously, the mountstats tool incorrectly parsed arguments that ended with the slash character (/). Consequently, the mountstats command failed when the directory name included a slash at the end. This bug has been fixed, and the mountstats command no longer fails in this scenario.

BZ#1194802

The rpc.mountd daemon contained memory leaks, which caused rpc.mountd to use an excessive amount of memory and an undue number of CPU cycles. With this update, several memory leaks identified by the Valgrind tool have been plugged, and the described problem no longer occurs.

BZ#1026446

Previously, when the "mount -o remount" command was used and the mount failed, no error message was displayed. With this update, a relevant error message is displayed in this scenario.

BZ#1164317

The rpc.mountd daemon did not correctly parse IP-restricted submount exports. As a consequence, some exports were not accessible when they should have been. This bug has been fixed, and exports are now accessible when appropriate.

Enhancement

BZ#1172827

The mountstats tool has been updated to include the latest upstream features and improve performance. Several new options have been introduced ("--file" or "-f", "--since" or "-S", "--raw" or "-R"), output of the iostat and nfsstat commands has been improved, and relevant manual pages have been updated.

Users of nfs-utils are advised to upgrade to these updated packages, which fix these bugs and add this enhancement. After installing this update, the nfs service will be restarted automatically.

7.137. nfs-utils-lib

7.137.1. RHBA-2015:1312 — nfs-utils-lib bug fix update

Updated nfs-utils-lib packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The nfs-utils-lib packages contain support libraries required by the programs in the nfs-utils packages.

Bug Fixes

BZ#1129792

Prior to this update, the libnfsidmap library used "nobody@DEFAULTDOMAIN" when performing name lookup, but this did not match the behavior of the rpc.idmapd daemon. As a consequence, the nfsidmap utility did not properly handle situations when "nobody@DEFAULTDOMAIN" did not directly map to any user or group on the system. With this update, libnfsidmap uses the "Nobody-User" and "Nobody-Group" values in the /etc/idmapd.conf file when the default "nobody" user and group are set, and the described problem no longer occurs.

BZ#1223465

The nss_getpwnam() function previously failed to find the intended password entry when the DNS domain name contained both upper-case and lower-case characters. This update ensures that character case is ignored when comparing domain names, and nss_getpwnam() is able to retrieve passwords as expected.

Users of nfs-utils-lib are advised to upgrade to these updated packages, which fix this bug.

7.138. nfs4-acl-tools

7.138.1. RHBA-2015:1340 — nfs4-acl-tools bug fix update

Updated nfs4-acl-tools packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The nfs4-acl-tools packages provide utilities for managing NFSv4 Access Control Lists (ACLs) on files and directories mounted on ACL-enabled NFSv4 file systems.

Bug Fix

BZ#1161164

Previously, the nfs4_setfacl and nfs4_getfacl commands ignored the DENY access control entry (ACE) for the DELETE, WRITE_OWNER, and NAMED_ATTRS permissions. A patch has been applied to fix this bug, and setting or viewing DENY ACE is no longer ignored.

Users of nfs4-acl-tools are advised to upgrade to these updated packages, which fix this bug.

7.139. ntp

7.139.1. RHSA-2015:1459 — Moderate: ntp security, bug fix, and enhancement update

Updated ntp packages that fix multiple security issues, several bugs, and add two enhancements are now available for Red Hat Enterprise Linux 6.

Red Hat Product Security 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 Network Time Protocol (NTP) is used to synchronize a computer's time with another referenced time source.

Security Fixes

CVE-2014-9298

It was found that because NTP's access control was based on a source IP address, an attacker could bypass source IP restrictions and send malicious control and configuration packets by spoofing ::1 addresses.

CVE-2015-1799

A denial of service flaw was found in the way NTP hosts that were peering with each other authenticated themselves before updating their internal state variables. An attacker could send packets to one peer host, which could cascade to other peers, and stop the synchronization process among the reached peers.

CVE-2015-3405

A flaw was found in the way the ntp-keygen utility generated MD5 symmetric keys on big-endian systems. An attacker could possibly use this flaw to guess generated MD5 keys, which could then be used to spoof an NTP client or server.

CVE-2014-9297

A stack-based buffer overflow was found in the way the NTP autokey protocol was implemented. When an NTP client decrypted a secret received from an NTP server, it could cause that client to crash.

CVE-2015-1798

It was found that ntpd did not check whether a Message Authentication Code (MAC) was present in a received packet when ntpd was configured to use symmetric cryptographic keys. A man-in-the-middle attacker could use this flaw to send crafted packets that would be accepted by a client or a peer without the attacker knowing the symmetric key.

The CVE-2015-1798 and CVE-2015-1799 issues were discovered by Miroslav Lichvár of Red Hat.

Bug Fixes

BZ#1053551

The ntpd daemon truncated symmetric keys specified in the key file to 20 bytes. As a consequence, it was impossible to configure NTP authentication to work with peers that use longer keys. The maximum length of keys has now been changed to 32 bytes.

BZ#1184421

The ntp-keygen utility used the exponent of 3 when generating RSA keys, and generating RSA keys failed when FIPS mode was enabled. ntp-keygen has been modified to use the exponent of 65537, and generating keys in FIPS mode now works as expected.

BZ#1045376

The ntpd daemon included a root delay when calculating its root dispersion. Consequently, the NTP server reported larger root dispersion than it should have and clients could reject the source when its distance reached the maximum synchronization distance (1.5 seconds by default). Calculation of root dispersion has been fixed, the root dispersion is now reported correctly, and clients no longer reject the server due to a large synchronization distance.

BZ#1171630

The ntpd daemon dropped incoming NTP packets if their source port was lower than 123 (the NTP port). Clients behind Network Address Translation (NAT) were unable to synchronize with the server if their source port was translated to ports below 123. With this update, ntpd no longer checks the source port number.

Enhancements

BZ#1122015

This update introduces configurable access of memory segments used for Shared Memory Driver (SHM) reference clocks. Previously, only the first two memory segments were created with owner-only access, allowing just two SHM reference clocks to be used securely on a system. Now, the owner-only access to SHM is configurable with the "mode" option, and it is therefore possible to use more SHM reference clocks securely.

BZ#1117704

Support for nanosecond resolution has been added to the SHM reference clock. Prior to this update, when a Precision Time Protocol (PTP) hardware clock was used as a time

source to synchronize the system clock (for example, with the timemaster service from the linuxptp package), the accuracy of the synchronization was limited due to the microsecond resolution of the SHM protocol. The nanosecond extension in the SHM protocol now enables sub-microsecond synchronization of the system clock.

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

7.140. numad

7.140.1. RHBA-2015:1441 — numad bug fix update

Updated numad packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The numad packages provide a daemon for Non-Uniform Memory Architecture (NUMA) systems, monitors NUMA characteristics, and manages placement of processes and memory to minimize memory latency. The packages also provide an interface that can be used to query the numad daemon for the best manual placement of an application.

Bug Fixes

BZ#1150585

Previously, the numad daemon could run out of file descriptors. When upgrading numad on KVM-Hypervisor, the following error messages were returned, after which numad terminated unexpectedly:

Could not write 1 to /cgroup/cpuset/libvirt/qemu/vm_name/emulator/cpuset.mems -- errno: 13

The underlying source code has been fixed, and numad no longer crashes in this situation.

BZ#1186724

Prior to this update, superfluous quotes in the numad initscript confused the daemon() function, which subsequently constructed a wrong argument. As a consequence, the following error message was returned:

Starting numad: /usr/bin/dirname: extra operand `-i' Try `/usr/bin/dirname --help' for more information.

A patch removing the quotes around daemon() parameters fixes this bug, and the error messages are no longer returned.

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

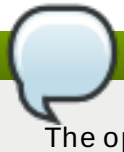
7.141. opencryptoki

7.141.1. RHBA-2015:1278 — opencryptoki bug fix and enhancement update

Updated opencryptoki packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The opencryptoki packages contain version 2.11 of the PKCS#11 API, implemented for IBM Cryptocards, such as IBM 4764 and 4765 crypto cards. These packages includes support for the IBM 4758 Cryptographic CoProcessor (with the PKCS#11 firmware loaded), the IBM eServer Cryptographic Accelerator (FC 4960 on IBM eServer System p), the IBM Crypto Express2 (FC 0863 or

FC 0870 on IBM System z), and the IBM CP Assist for Cryptographic Function (FC 3863 on IBM System z). The opencryptoki packages also bring a software token implementation that can be used without any cryptographic hardware. These packages contain the Slot Daemon (pkcsslotd) and general utilities.



Upgrade to an upstream version

The opencryptoki packages have been upgraded to upstream version 3.2, which provides a number of bug fixes and enhancements over the previous version. (BZ#1148134)

Enhancements

BZ#1148734

This update enables Central Processors Assist for Cryptographic Functions (CPACF) Message Security Assist 4 (MSA-4) extensions with new modes of operation for opencryptoki on IBM System z. In addition, this hardware encryption improves performance on machines z196 and later.

BZ#11148133

This update also implements an opencryptoki token for access to the Enterprise PKCS#11 (EP11) features of the Crypto Express4S (CEX4S) adapter that implements certified PKCS#11 mechanism on IBM System z.

Users of opencryptoki are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.142. openhpi32

7.142.1. RHBA-2015:1449 — openhpi32 bug fix and enhancement update

Updated openhpi32 packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

OpenHPI is an open source project created with the intent of providing an implementation of the SA Forum's Hardware Platform Interface (HPI). HPI provides an abstracted interface to managing computer hardware, typically for chassis and rack based servers. HPI includes resource modeling; access to and control over sensor, control, watchdog, and inventory data associated with resources; abstracted System Event Log interfaces; hardware events and alerts; and a managed hot swap interface.

Upgrade to an upstream version

The openhpi32 packages have been upgraded to upstream version 3.4.0, which provides a number of bug fixes and enhancements over the previous version. (BZ#1127907)

Bug Fixes

BZ#1127907

Encryption of the configuration file is now allowed, so authentication credentials for hardware management are no longer available in clear text on the system.

Support for IPv6 has been fixed in the Onboard Administrator (OA) SOAP plug-in.

The uid_map file is no longer created as world-writable.

BZ#1069015

Prior to this update, a data race condition was present in the Intelligent Platform Management Interface (IPMI) plug-in within the multi-threaded daemon. Consequently, the openhpid daemon could terminate unexpectedly with a segmentation fault. This bug has been fixed, the data structures are now updated in the correct order, and openhpid no longer crashes in this scenario.

BZ#1105679

Network timeouts were handled incorrectly in the openhpid daemon. As a consequence, network connections could fail when external plug-ins were used. With this update, handling of network socket timeouts has been improved in openhpid, and the described problem no longer occurs.

Users of openhpi32 are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.143. openjpeg

7.143.1. RHBA-2014:2001 — openjpeg bug fix update

Updated openjpeg packages that fix one bug are now available for Red Hat Enterprise Linux 6.

OpenJPEG is an open source library for reading and writing image files in JPEG 2000 format.

Bug Fix

BZ#1047494

Due to a regression introduced in the previous version of the openjpeg packages, chroma-subsampled images became corrupted during decoding. An upstream patch has been applied to fix this bug, and the images are now decoded correctly.

Users of openjpeg are advised to upgrade to these updated packages, which fix this bug. All running applications using OpenJPEG must be restarted for the update to take effect.

7.144. openldap

7.144.1. RHBA-2015:1292 — openldap bug fix and enhancement update

Updated openldap packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

OpenLDAP is an open-source suite of Lightweight Directory Access Protocol (LDAP) applications and development tools. LDAP is a set of protocols used to access and maintain distributed directory information services over an IP network. The openldap packages contain configuration files, libraries, and documentation for OpenLDAP.

Upgrade to an upstream version

The openldap packages have been upgraded to upstream version 2.4.40, which provides a number of bug fixes and enhancements over the previous version. (BZ#1147983)

Bug Fixes

BZ#1144294

Previously, openldap did not correctly handle when multiple processes attempted to establish an encrypted connection at the same time. Consequently, utilities, such as the nslcd service, could terminate unexpectedly with a segmentation fault. Incorrect thread initialization code that caused this bug has been fixed. As a result, utilities no longer crash when processes establish multiple concurrent encrypted connections.

BZ#1164369

Previously, the server could terminate unexpectedly when processing SRV records due to invalid memory access. The error that caused the invalid memory access has been corrected, and the server no longer crashes when processing SRV records.

BZ#1193519

Prior to this update, user data was deleted after updating openldap when the slapd.conf file was used to store the configuration, but the slapd.d/ directory also existed. This update fixes incorrect logic in the post-installation script, and user data is no longer deleted in this situation.

BZ#1202696

The server sometimes terminated unexpectedly with a segmentation fault on IBM Power Systems due to a regression. A code optimization that caused this problem has been removed, preventing the segmentation fault from occurring. As a result, the server no longer crashes in this situation.

Enhancements

BZ#1155390

This update introduces the Check Password extension for OpenLDAP, required for PCI compliance.

BZ#1160467

Support for the TLS protocol version 1.1 and later has been added.

Users of openldap are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.145. openscap

7.145.1. RHBA-2015:1317 — openscap bug fix and enhancement update

Updated openscap packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

OpenSCAP is an open source project, which enables integration of the Security Content Automation Protocol (SCAP) line of standards. SCAP is a line of standards managed by the National Institute of Standards and Technology (NIST). It was created to provide a standardized approach to maintaining the security of enterprise systems, such as automatically verifying presence of patches, checking system security configuration settings, and examining systems for signs of compromise.

Upgrade to an upstream version

The openscap packages have been upgraded to upstream version 1.0.10, which provides a number of bug fixes and enhancements over the previous version. Updated version is fully API/ABI compatible with 1.0.x version which has been certified by the National Institute of Standards and Technology (NIST). (BZ#1152599)

Bug Fixes

BZ#1036741

Previously, the has_extended_acl feature was missing in the scripts that build OpenSCAP, which caused the OpenSCAP auditing tool to be unable to assess extended file system properties. This update fixes the build process of OpenSCAP to include has_extended_acl, and OpenSCAP is now again able to assess extended file system properties as intended.

BZ#1092013

When the Extensible Configuration Checklist Description Format (XCCDF) input content included an instruction to use a certain XCCDF variable with an undefined variable value, the OpenSCAP scanner could crash. With this update, the NULL pointer causing this bug is handled correctly when binding the XCCDF value to the OVAL variable, and the security scan now proceeds smoothly.

BZ#1192428

The OVAL standard requires that the var_check content XML attribute be included within any XML elements that have the var_ref attribute, which the OpenSCAP scanner did not always observe. As a consequence, the schematron validation of OVAL results returned a warning message to the user. The OVAL module has been fixed to export var_check explicitly whenever exporting var_ref, and the schematron validation now passes as expected.

Enhancement

BZ#1115114

To keep the installed package set to the minimum, the number of package dependencies of the OpenSCAP auditing tool has been reduced. With this update, the oscap tool is shipped within the newly created openscap-scanner package and the openscap-utils package remains to include miscellaneous tools. Users are advised to remove openscap-utils, if they no longer need other utilities except for the scanner.

Users of openscap are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.146. openssh

7.146.1. RHBA-2015:1335 — openssh bug fix and enhancement update

Updated openssh packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

OpenSSH is OpenBSD's SSH (Secure Shell) protocol implementation. These packages include the core files necessary for both the OpenSSH client and server.

Bug Fixes

BZ#1085710

Every first attempt to make a connection using the sftp utility, before the user information was stored in the System Security Services Daemon (SSSD) cache, failed. The sshd server no longer closes file descriptors before all the user information is loaded, and sftp connections in combination with SSSD work even when the SSSD cache is empty. Now, first sftp connection attempts succeed.

BZ#1093869

Printing extensions for v01 certificates using the "ssh-keygen -L -f" command did not display the certificate extensions correctly. Now, printing extensions for v01 certificates works as expected.

BZ#1109251

The sshd configuration test mode, executed by the "sshd -T" command, did not display all default options and displayed certain other options incorrectly. With this update, the sshd test mode outputs all required default options and also prints the above-mentioned other options correctly. Output of the configuration test mode can be now safely applied as configuration input.

BZ#1127312

Non-existing users logging in with ssh triggered two different audit messages in the log, which was not expected behavior. With this update, when a non-existing user attempts to log in using ssh, only one audit message is triggered. This message records a login attempt from an unknown user as expected.

BZ#1131585

When the ForceCommand option with a pseudoterminal was used and the MaxSession option was set to "2", multiplexed ssh connections did not work as expected. After the user attempted to open a second multiplexed connection, the attempt failed if the first connection was still open. This update modifies OpenSSH to issue only one audit message per session. The user is able to open two multiplexed connections in this situation.

BZ#1134938

Previously, OpenSSH did not correctly handle quoted multiple values defined on one configuration line. When the user specified, for example, multiple groups in quotes on one line, OpenSSH only honored the first specified group. The OpenSSH configuration parser has been modified, and OpenSSH honors all option values in this situation.

BZ#1135521

The ssh-copy-id utility failed if the account on the remote server did not use an sh-like shell. Remote commands have been modified to run in an sh-like shell, and ssh-copy-id now also works with non-sh-like shells.

BZ#1161454

The user could not generate ssh keys on hosts with a host name of 64 characters. The ssh-keygen utility failed in this situation. The buffer size for host names has been increased, and ssh-keygen no longer fails in the described situation.

BZ#1172224

All the messages obtained from an sftp server when using chroot were logged in the global log file through the sshd server even when a valid socket for logging was available. Now, events from the sftp server can be logged through the socket in chroot and forwarded into an independent log file.

BZ#1196331

The ssh-keyscan command did not scan for Elliptic Curve Digital Signature Algorithm (ECDSA) keys. The "ssh-keyscan -t ecdsa -v localhost" command did not display any output. The command now outputs the host ECDSA key as expected.

BZ#1208584

This update fixes memory leaks discovered in sshd.

Enhancements

BZ#1119506

This update adds support for adjusting LDAP queries. The administrator can adjust the LDAP query to obtain public keys from servers that use a different schema.

BZ#1159055

The PermitOpen option in sshd_config file now supports wildcards.

BZ#1191055

With this update, openssh can force exact permissions on files that are newly uploaded using sftp.

Users of openssh are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.147. openssl

7.147.1. RHBA-2015:1398 — openssl bug fix and enhancement update

Updated openssl packages that fix two bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

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.

Bug Fixes

BZ#1119191

Previously, the ciphers(1) manual page did not describe the following Elliptic Curve Cryptography (ECC) cipher suite groups: Elliptic Curve Diffie–Hellman (ECDH) and Elliptic

Curve Digital Signature Algorithm (ECDSA), or TLS version 1.2 (TLSv1.2) specific features. This update adds the missing description of the ECDH and ECDSA cipher groups and TLSv1.2 features to ciphers(1), and the documentation is now complete.

BZ#1234487

The server-side renegotiation support did previously not work as expected under certain circumstances. A PostgreSQL failure of database dumps through TLS connection could occur when the size of the dumped data was larger than the value defined in the ssl_renegotiation_limit setting. The regression that caused this bug has been fixed, and the PostgreSQL database dumps through TLS connection no longer fail in the described situation.

Enhancement

BZ#961965

This update adds the "-keytab" option to the "openssl s_server" command and the "-krb5svc" option to the "openssl s_server" and "openssl s_client" commands. The "-keytab" option allows the user to specify a custom keytab location; if the user does not add "-keytab", the openssl utility assumes the default keytab location. The "-krb5svc" option enables selecting a service other than the "host" service; this allows unprivileged users without keys to the host principal to use "openssl s_server" and "open s_client" with Kerberos.

Users of openssl are advised to upgrade to these updated packages, which fix these bugs and add this enhancement. For the update to take effect, all services linked to the OpenSSL library must be restarted, or the system rebooted.

7.148. openssl-ibmca

7.148.1. RHBA-2015:0792 — openssl-ibmca bug fix update

Updated openssl-ibmca packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The openssl-ibmca packages provide a dynamic OpenSSL engine for the IBM eServer Cryptographic Accelerator (ICA) crypto hardware on IBM eServer zSeries machines.

Bug Fixes

BZ#1075183

Prior to this update, an incorrect flag was passed to the elliptic curve crypto signing method. Consequently, the selftest in the OpenSSL library failed when the IBMCA engine was in use. Now, the correct flag is passed, and the OpenSSL selftest succeeds.

BZ#1193071

Previously, the IBMCA engine truncated the SHA256 hash data computed by the Library for IBM Cryptographic Architecture (libica). As a consequence, the certificate verification process used a malformed hash and failed. Now, the correct length is used for the SHA256 data, and certificate verification proceeds without errors.

Users of openssl-ibmca are advised to upgrade to these updated packages, which fix these bugs.

7.149. oprofile

7.149.1. RHBA-2015:1367 — oprofile bug fix and enhancement update

Updated oprofile packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

OProfile is a low-overhead, system-wide profiler that uses the performance monitoring hardware on the processor to retrieve information about the kernel and executables on the system.

Bug Fixes

BZ#1180513

Previously, when profiling performance of Java just-in-time (JIT) compiled code with static huge pages enabled, OProfile's operf command recorded a large number of event samples to anonymous memory (in anon_hugepage) instead of to the appropriate Java method. With this update, operf recognizes the static huge page identifiers and correctly maps samples to Java methods when using statically allocated huge pages.

BZ#1199469

To properly select an event, some new Intel processors require not only the base event number but also additional bits to be set in the unit mask. Previously, the additional bits in the unit mask remained unset, thus being incorrectly set to zero. As a consequence, performance monitoring hardware was not measuring the desired event, and the operf utility returned zero for the LLC_REFS and LLC_MISSES events on the 2nd, 3rd, and 4th generation Intel Core and Intel Xeon processors. With this update, OProfile code has been fixed to set the unit mask bits as required. As a result, performance events on Intel processors that require non-zero unit masks now work as expected.

BZ#1200808

Previously, when a name of the default unit mask for an event was longer than 11 characters, OProfile truncated the name to 11 characters. Consequently, when the truncated unit mask name was used, OProfile could not find the unit mask and returned an error message. With this update, OProfile handles long unit mask names correctly, and the described problem no longer occurs.

BZ#1202727

The operf, ocount, and opjitconv utilities set the POSIXLY_CORRECT enviroment variable for their internal purposes. Prior to this update, OProfile did not return this environment variable to its previous state, thus potentially affecting profiled tasks. Consequently, profiled tasks that behaved differently when the variable was set, such as rpm rebuilds, did not work as expected. This bug has been fixed, and the OProfile use of POSIXLY_CORRECT now does not affect profiled tasks.

Enhancement

BZ#1144235

The OProfile profiler tool now includes support for Intel Silvermont events for the Intel Atom C2XXX and Intel Atom E38XX systems on a chip (SoC). This allows users to investigate Intel Silvermont-specific performance issues using OProfile.

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

7.150. pacemaker

7.150.1. RHSA-2015:1424 — Moderate: pacemaker security and bug fix update

Updated pacemaker packages that fix one security issue and several bugs are now available for Red Hat Enterprise Linux 6.

Red Hat Product Security 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 Pacemaker Resource Manager is a collection of technologies working together to provide data integrity and the ability to maintain application availability in the event of a failure.

Security Fix

CVE-2015-1867

A flaw was found in the way pacemaker, a cluster resource manager, evaluated added nodes in certain situations. A user with read-only access could potentially assign any other existing roles to themselves and then add privileges to other users as well.

Bug Fixes

BZ#1198638

Due to a race condition, nodes that gracefully shut down occasionally had difficulty rejoining the cluster. As a consequence, nodes could come online and be shut down again immediately by the cluster. This bug has been fixed, and the "shutdown" attribute is now cleared properly.

BZ#1205292

Prior to this update, the pacemaker utility caused an unexpected termination of the attrd daemon after a system update to Red Hat Enterprise Linux 6.6. The bug has been fixed so that attrd no longer crashes when pacemaker starts.

BZ#1207621

Previously, the access control list (ACL) of the pacemaker utility allowed a role assignment to the Cluster Information Base (CIB) with a read-only permission. With this update, ACL is enforced and can no longer be bypassed by the user without the write permission, thus fixing this bug.

BZ#1208896

Prior to this update, the ClusterMon (crm_mon) utility did not trigger an external agent script with the "-E" parameter to monitor the Cluster Information Base (CIB) when the pacemaker utility was used. A patch has been provided to fix this bug, and crm_mon now calls the agent script when the "-E" parameter is used.

Users of pacemaker are advised to upgrade to these updated packages, which contain backported patches to correct these issues.

7.151. pam_passwdqc

7.151.1. RHBA-2015:0712 — pam_passwdqc bug fix update

Updated pam_passwdqc packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The pam_passwdqc packages provide a simple password strength checking module for PAM (Pluggable Authentication Module) aware password changing programs, such as passwd(1). In addition to checking regular passwords, the module offers support for passphrases and can provide randomly generated passwords. All the features of the module are optional and can be reconfigured without rebuilding.

Bug Fix

BZ#889545

Previously, the pam_passwdqc man page contained an unclear description of the relationship between the minimum password length and complexity. Consequently, users of this PAM module reading the man page could misinterpret the actual requirements for sufficiently secure passwords. With this update, a detailed description of the required password complexity for various lengths has been provided in the man page, and as a result, the documentation is no longer ambiguous.

Users of pam_passwdqc are advised to upgrade to these updated packages, which fix this bug.

7.152. papi

7.152.1. RHEA-2015:1313 — papi enhancement update

Updated papi packages that add one enhancement are now available for Red Hat Enterprise Linux 6.

PAPI (Performance Application Programming Interface) is a software library that provides a specification of cross-platform interfaces to hardware performance counters on modern microprocessors. These counters exist as a small set of registers that count events, which are occurrences of specific signals related to a processor's function. Monitoring these events allows developers to track performance-related events, such as cache misses, instructions retired, and clock cycles, to better understand the performance issues of the software. PAPI uses libpfm to select the performance monitoring events for the various processors.

Enhancement

BZ#831752

The support for Intel Core and Intel Xeon v3 family processors, as well as certain Intel Pentium and Intel Celeron family processors, has been added to PAPI. As a result, developers can now use PAPI on machines with the these processors. Note that this feature has been added only to version 5 of PAPI. For the PAPI 4 libraries, included in the packages for compatibility, these processors remain unsupported.

Users of papi are advised to upgrade to these updated packages, which add this enhancement.

7.153. parted

7.153.1. RHBA-2015:1357 — parted bug fix update

Updated parted packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The parted packages provide tools to create, destroy, resize, move, and copy hard disk partitions. The parted program can be used for creating space for new operating systems, reorganizing disk usage, and copying data to new hard disks.

Bug Fixes

BZ#1189328

Partitions that parted created while operating on device-mapper devices, such as mpath, could be smaller than expected. This update modifies parted to convert the native device sector size to 512 sector size when communicating with the device-mapper library. As a result, partitions are created with the correct size in the mentioned situation.

BZ#1180683

Previously, parted did not correctly handle disks or disk images where the backup GUID Partition Table (GPT) header was missing or could not be found at the expected location at the end of the disk. This situation can occur with disks that are shorter or longer than when they were originally created. Consequently, parted could terminate unexpectedly or prompt the user to have parted fix the problem and fail to do so. A patch has been applied to fix GPT backup header handling. Now, after the user instructs parted to fix the problem in the described scenario, parted succeeds.

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

7.154. pcp

7.154.1. RHBA-2015:1300 — pcp bug fix and enhancement update

Updated pcp packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

Performance Co-Pilot (PCP) is a suite of tools, services, and libraries for acquisition, archiving, and analysis of system-level performance measurements. Its light-weight, distributed architecture makes it particularly well-suited to centralized analysis of complex systems.

Upgrade to an upstream version

The pcp packages have been upgraded to upstream version 3.10.3, which provides numerous bug fixes and enhancements over the previous version. (BZ#1158681)

Bug Fixes

BZ#1158681

New kernel metrics: memory, vCPU, device mapper, nfs4.1 operations, more per-cgroup metrics

- New Performance Metrics Domain Agents (PMDA): NVIDIA, Linux, 389 Directory Server, hardware event counters, CIFS, activeMQ
- New vCPU and MemAvailable pmchart views
- New pmiostat, pcp-dmcache, pcp2graphite, ganglia2pcp tools
- Nanosecond resolution event timestamps
- The pmParseUnitsStr() function added to the Performance Metrics Application Programming Interface (PMAPI)

- ACAO header JSON responses added to the Performance Metrics Web Daemon (pmwebd)
- The "ruleset" extensions to the pmie language
- Support for Python v3 and Python API extensions
- Support for xz compression for daily archives
- Support for long form of command-line options
- Support for active service probing in libpcp
- Support for new sysstat versions and sar2pcp fixes
- Direct support for PCP archive in the pmatop utility

BZ#1196540

Previously, on IBM S/390 platforms, unanticipated formatting in the /proc/cpuinfo file negatively affected the PCP Linux kernel PMDA. As a consequence, the agent terminated unexpectedly with a segmentation fault when accessing certain processor related performance metrics. This update fixes parsing of /proc/cpuinfo for IBM S/390, and all PCP processor metrics are now fully functional and robust on this platform.

BZ#1131022

Previously, the PCP pmlogger daemon start script started the daemon only if the pmlogger service was enabled by the "chkconfig on" command. Consequently, the daemon silently failed to start when the service was disabled. With this update, additional diagnostics have been added to the start script. Now, when attempting to start the pmlogger daemon with the pmlogger service disabled, the user is properly informed and given instructions on how to eliminate the problem.

Users of pcp are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.155. pcre

7.155.1. RHEA-2015:1374 — pcre enhancement update

Updated pcre packages that add one enhancement are now available for Red Hat Enterprise Linux 6.

PCRE is a Perl-compatible regular expression library.

Enhancement

BZ#1193524

To allow the grep utility to recover from PCRE matching failures if the binary file is not a valid UTF-8 sequence, the following features have been backported to the PCRE library:

- The pcre_exec() function now checks for out-of-range starting offset values and reports PCRE_ERROR_BADOFFSET errors instead of reporting PCRE_ERROR_NOMATCH errors or looping infinitely.

- If the pcre_exec() function is called to perform a UTF-8 match on an invalid UTF-8 subject string and the ovector array argument is large enough, the offset of the first subject string in

the invalid UTF-8 byte, as well as the detailed reason code, are returned in the ovector array element. In addition, the "pcretest" utility can now be used to display these details. Note that with this update, the pcre_compile() function reports first invalid UTF-8 byte instead of the last byte.

Also note that the signature of the pcre_valid_utf8() function, which is not intended for public use, has been changed. Finally, note that "pcretest" now appends human-readable error messages to error codes.

Users of pcre are advised to upgrade to these updated packages, which add this enhancement.

7.156. pcs

7.156.1. RHBA-2015:1446 — pcs bug fix and enhancement update

Updated pcs packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The pcs packages provide a command-line configuration system for the Pacemaker and Corosync utilities.

Upgrade to an upstream version

The pcs packages have been upgraded to upstream version 0.9.139, which provides a number of bug fixes and enhancements over the previous version. (BZ#1185738)

Bug Fixes

BZ#1031141

After the user added a duplicate resource operation, Pacemaker configuration became invalid. With this update, pcs does not add the operation and instead informs the user that the same operation already exists.

BZ#1160359

The user could not manage Red Hat Enterprise Linux 6 clusters using the pcsd web UI running on a Red Hat Enterprise Linux 7 host. The bug has been fixed, and it is now possible to add or create clusters in this situation. Note that the pcsd web UI is still not available on Red Hat Enterprise Linux 6 hosts.

BZ#1174244

After the user displayed the list of STONITH devices or resources, their locations were not included. Now, the list also contains the locations of the devices and resources.

BZ#1174793

The "pcs resource describe" command displayed the resource agent description on one line, which made it difficult to read. Now, pcs displays the description as it is defined in the agent.

BZ#1174798

After displaying information about a fence agent, pcs showed the description of the options but not the description of the fence agent itself. Now, the fence agent description is displayed as well in this situation.

BZ#1174801, BZ#1184763

Previously, pcs stopped cluster nodes sequentially one at a time, which caused the cluster resources to be moved from one node to another pointlessly. Consequently, the stop operation took a long time to finish. Also, losing the quorum during the process could result in node fencing. With this update, pcs stops the nodes simultaneously, preventing the resources from being moved around pointlessly and speeding up the stop operation. In addition, pcs prints a warning if stopping the nodes would cause the cluster to lose the quorum. To stop the nodes in this situation, the user is required to add the "--force" option.

BZ#1184922, BZ#1187488

The "pcs status --full" command did not output the node attributes and migration summary. Similarly, the "pcs config" command did not display the resource and operation defaults. Both commands have been modified to display this information.

BZ#1190167

After the user attempted to ban or clear a clone resource, pcs displayed an error message stating the resource did not exist. With this update, pcs supports banning and clearing clone resources. The "pcs resource ban" command creates a constraint on a cloned resource, and the "pcs resource clear" command removes that constraint.

BZ#1191898

When using the User Datagram Protocol unicast (UDPU) transport, the cluster is required to be restarted in order for the node to be added or removed properly. Previously, pcs did not inform the user about this requirement. Now, pcs warns the user to restart the cluster.

BZ#1193433

After the user removed a node from a cluster, the cluster could fence the removed node. This update modifies pcs to reload the cluster.conf file after adding or removing a node, thus fixing the bug.

Enhancements

BZ#1121769

This update adds support for configuring the Redundant Ring Protocol (RRP) and setting Corosync options. The user can now configure a cluster with RRP and set up corosync options.

BZ#1171312

The clufter package is now installed as a pcs dependency. With clufter installed, pcs is able to import CMAN configuration from the cluster.conf file and convert it into Pacemaker configuration.

Users of pcs are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.157. pcsc-lite

7.157.1. RHBA-2015:1369 — pcsc-lite bug fix update

Updated pcsc-lite packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

PC/SC Lite provides a Windows SCard compatible interface for communicating with smart cards, smart card readers, and other security tokens.

Bug Fixes

BZ#956530

Previously, after a card reader went offline when the user entered the settings menu, the pcsc-lite client could under certain circumstances enter a deadlock state and never recover from it. The underlying source code has been modified so that the client does not wait for an unreleased mutex. As a result, the client does not enter a deadlock state in the described situation, and the reader is accessible again after it returns online.

BZ#1171118

On systems with the pcsc-lite-openct package uninstalled, if the pcscd service terminated unexpectedly or was killed, restarting or stopping and starting pcscd failed. This update modifies pcscd to remove the pcscd.comm and pcscd.pub files after pcscd terminates unexpectedly or is killed. As a result, pcscd can be restarted or stopped and started again as expected in the described situation.

Users of pcsc-lite are advised to upgrade to these updated packages, which fix these bugs.

7.158. perl

7.158.1. RHBA-2015:1266 — perl bug fix update

Updated perl packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

Perl is a high-level programming language that is commonly used for system administration utilities and web programming.

Bug Fixes

BZ#1104827

Due to creating threads after tying a variable to an SDBM database using the SDBM_File Perl module, the Perl interpreter terminated unexpectedly when terminating Perl threads. With this update, the DB_File, GDBM_File, NDBM_File, ODBM_File, and SDBM_File Perl modules have been modified to destroy their objects only from the thread context which created the objects. As a result, the destructors of the aforementioned file objects are now thread-safe. Note, however, that other operations on the objects cannot be called from other threads. In general, the DB_File, GDBM_File, NDBM_File, ODBM_File, and SDBM_File Perl modules remain thread-unsafe.

BZ#1086215

Previously, using the Module::Pluggable Perl module to locate plug-ins in a single-letter-named package did not work correctly. As a consequence, existing single-letter-named packages were not found. An upstream patch has been applied, and single-letter-named plug-ins are now located by Module::Pluggable correctly.

BZ#1161170

Previously, the perl-suidperl package consumed the libperl.so library from the perl-libs subpackage with no explicit package-version requirement. This could cause problems, for example, during upgrading. With this update, an explicit dependency on the same version of perl-libs has been added to perl-suidperl, which avoids accidental mixing of incompatible perl-suidperl and perl-libs packages on a system.

BZ#1025906

The Perl Locale::Maketext localization framework did not properly translate the backslash (\) characters. As a consequence, Perl rendered the backslashes as double (\\). With this update, Perl no longer escapes the backslashes in literal output strings, and they appear correctly.

BZ#1184194

Prior to this update, the Archive::Tar Perl module unpacked PAX headers into artificial PaxHeader subdirectories, which caused the extracted tree to be different from the archived tree. Consequently, installation of a Comprehensive Perl Archive Network (CPAN) distribution by the cpan client failed. This bug has been fixed, and it is now possible to install CPAN distributions archived with extended attributes.

BZ#1189041

Previously, when the SHA::Digest method was called on the corresponding class, Perl terminated unexpectedly with a segmentation fault. An upstream patch has been applied, and calling any SHA::Digest method on a class yields a proper exception instead of Perl crash.

BZ#1201191

Previously, due to earlier problems with threads, several tests were blocked for IBM S/390, IBM System z, or PowerPC platforms in the Perl specification file. Consequently, when building the perl package, internal tests were not performed on these platforms, even though the original problems no longer occurred. Now, when building the perl package, the tests are performed on all supported architectures.

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

7.159. perl-Sys-Virt

7.159.1. RHBA-2015:1387 — perl-Sys-Virt bug fix update

Updated perl-Sys-Virt packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The Sys::Virt module provides a Perl XS binding to the libvirt virtual machine management APIs. This allows machines running within arbitrary virtualization containers to be managed with a consistent API.

Bug Fixes

BZ#905836

Previously, using the libvirt-tck utility to display virtual CPU (VCPU) information only printed a part of the expected diagnostics. With this update, the get_vcpu_info() function handles VCPU flags properly, and libvirt-tck displays the full extent of the expected information.

BZ#908274

Prior to this update, using the libvirt-tck utility to find the parent device of a node device with no parent incorrectly returned a "libvirt error code: 0" error message. Now, it is valid for the virNodeDeviceGetParent() function to return NULL if the parent device is nonexistent, and the error message is no longer displayed.

Users of perl-Sys-Virt are advised to upgrade to these updated packages, which fix these bugs.

7.160. pinentry

7.160.1. RHBA-2015:0755 — pinentry bug fix update

Updated pinentry packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The pinentry packages contain a collection of simple personal identification number (PIN) or password entry dialogs, which utilize the Assuan protocol as described by the Project Aegypten. The pinentry packages also contain the command line version of the PIN entry dialog.

Bug Fixes

BZ#662770

Due to an auto-detection problem, the pinentry wrapper in some cases attempted to launch the pinentry-gtk program even if it was not installed. The pinentry wrapper has been updated, and the problem no longer occurs.

BZ#704495

Due to lack of UTF-8 support, the output description text got scrambled when the "pinentry getpin" command was used. The same problem could occur when using the GNU Privacy Guard utility that called the "pinentry getpin" command on a key containing non-ASCII characters in its name. To fix this bug, proper UTF-8 translation has been performed, and the pinentry-curses binary file has been compiled against the ncursesw library, which contains wide character support. As a result, the output text is now correct.

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

7.161. pki-core

7.161.1. RHSA-2015:1347 — Moderate: pki-core security and bug fix update

Updated pki-core packages that fix one security issue and several bugs are now available for Red Hat Enterprise Linux 6.

Red Hat Product Security 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 Certificate System is an enterprise software system designed to manage enterprise public key infrastructure (PKI) deployments. PKI Core contains fundamental packages required by Red Hat Certificate System, which comprise the Certificate Authority (CA) subsystem.

Security Fix

CVE-2012-2662

Multiple cross-site scripting flaws were discovered in the Red Hat Certificate System Agent

and End Entity pages. An attacker could use these flaws to perform a cross-site scripting (XSS) attack against victims using the Certificate System's web interface.

Bug Fixes

BZ#1171848

Previously, pki-core required the SSL version 3 (SSLv3) protocol ranges to communicate with the 389-ds-base packages. However, recent changes to 389-ds-base disabled the default use of SSLv3 and enforced using protocol ranges supported by secure protocols, such as the TLS protocol. As a consequence, the CA failed to install during an Identity Management (IdM) server installation. This update adds TLS-related parameters to the server.xml file of the CA to fix this problem, and running the ipa-server-install command now installs the CA as expected.

BZ#1212557

Previously, the ipa-server-install script failed when attempting to configure a stand-alone CA on systems with OpenJDK version 1.8.0 installed. The pki-core build and runtime dependencies have been modified to use OpenJDK version 1.7.0 during the stand-alone CA configuration. As a result, ipa-server-install no longer fails in this situation.

BZ#1225589

Creating a Red Hat Enterprise Linux 7 replica from a Red Hat Enterprise Linux 6 replica running the CA service sometimes failed in IdM deployments where the initial Red Hat Enterprise Linux 6 CA master had been removed. This could cause problems in some situations, such as when migrating from Red Hat Enterprise Linux 6 to Red Hat Enterprise Linux 7. The bug occurred due to a problem in a previous version of IdM where the subsystem user, created during the initial CA server installation, was removed together with the initial master. This update adds the restore-subsystem-user.py script that restores the subsystem user in the described situation, thus enabling administrators to create a Red Hat Enterprise Linux 7 replica in this scenario.

BZ#1144188

Several Java import statements specify wildcard arguments. However, due to the use of wildcard arguments in the import statements of the source code contained in the Red Hat Enterprise Linux 6 maintenance branch, a name space collision created the potential for an incorrect class to be utilized. As a consequence, the Token Processing System (TPS) rebuild test failed with an error message. This update addresses the bug by supplying the fully named class in all of the affected areas, and the TPS rebuild test no longer fails.

BZ#1144608

Previously, pki-core failed to build with the rebased version of the CMake build system during the TPS rebuild test. The pki-core build files have been updated to comply with the rebased version of CMake. As a result, pki-core builds successfully in the described scenario.

Users of pki-core are advised to upgrade to these updated packages, which contain backported patches to correct these issues.

7.162. policycoreutils

7.162.1. RHBA-2015:1360 — policycoreutils bug fix update

Updated policycoreutils packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The policycoreutils packages contain the core utilities that are required for the basic operation of a Security-Enhanced Linux (SELinux) system and its policies.

Bug Fixes

BZ#995778

Previously, the sepolgen utility was a part of the policycore-gui package, even though it does not require any GUI. With this update, sepolgen is a part of the policycore-python package.

BZ#1111999

The "audit2allow -br" command did not work properly when the "LANG" environment variable was set to a different language than "US/English". The underlying source code has been modified, and "audit2allow -br" now works as expected.

BZ#1113083

When running the fixfiles utility in "verify" or "check" mode, fixfiles changed certain SELinux contexts even if it was not supposed to. With this update, fixfiles has been modified to only print incorrect SELinux contexts instead of changing them when running in aforementioned modes.

BZ#1122850

The semanage utility previously listed only changes made to the currently used SELinux policy. For example, when the targeted policy was loaded and changes were made to the Multi-Level Security (MLS) policy, the "semanage -S mls -o" command did not list all the changes, even when the changes were applied correctly. This bug has been fixed, and semanage now lists all changes as expected.

BZ#1148062

A new "noreload" option was implemented for semanage commands in Red Hat Enterprise Linux 6.6. However, due to a missing reload initialization in the semanageRecords() function, users could not enable Booleans directly using the seobject python module that comes from the policycoreutils-python utility. This bug has been fixed, and users can now set Booleans correctly using the seobject python module.

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

7.163. polkit

7.163.1. RHBA-2015:0692 — polkit bug fix update

Updated polkit packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

PolicyKit is a toolkit for defining and handling authorizations. It is used for allowing unprivileged processes to speak to privileged processes.

Bug Fixes

BZ#1115649

Prior to this update, the polkitd daemon was not restarted after upgrading the polkit package, nor stopped after the package uninstallation. To fix this bug, scriptlets have been added to the polkit package. Upgrading the polkit package to the version shipped in this erratum does not yet restart the polkitd daemon. The daemon will be restarted after future upgrades from this version.

BZ#1130156

Previously, the output of "pkcheck --help" did not match the supported arguments and their expected form. This update removes the unimplemented "--list-temp" option from "pkcheck --help", and fixes other aspects of the text as well.

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

7.164. powerpc-utils

7.164.1. RHBA-2015:1319 — powerpc-utils bug fix and enhancement update

Updated powerpc-utils packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The powerpc-utils packages provide various utilities for the PowerPC platform.

Enhancement

BZ#11248741

It is no longer possible for the "drmgr" command to erroneously remove the last CPU. * Support for up to eight threads in simultaneous multithreading (SMT) has been added. * It is possible to convert an Open Firmware (OF) device path to a logical device path for a virtio SCSI device. * The "snap" command now also warns about possible clear-text password disclosure.

Users of powerpc-utils are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.165. ppc64-diag

7.165.1. RHSA-2015:1320 — Moderate: ppc64-diag security, bug fix and enhancement update

Updated ppc64-diag packages that fix two security issues, several bugs, and add various enhancements are now available for Red Hat Enterprise Linux 6.

Red Hat Product Security 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 ppc64-diag packages provide diagnostic tools for Linux on the 64-bit PowerPC platforms. The platform diagnostics write events reported by the firmware to the service log, provide automated responses to urgent events, and notify system administrators or connected service frameworks about the reported events.

Security Fix

CVE-2014-4038, **CVE-2014-4039**

Multiple insecure temporary file use flaws were found in the way the ppc64-diag utility created certain temporary files. A local attacker could possibly use either of these flaws to perform a symbolic link attack and overwrite arbitrary files with the privileges of the user running ppc64-diag, or obtain sensitive information from the temporary files.

The ppc64-diag packages have been upgraded to upstream version 2.6.7, which provides a number of bug fixes and enhancements over the previous version. (BZ#1148142)

Bug Fixes

BZ#1139655

Previously, the "explain_syslog" and "syslog_to_svclog" commands failed with a "No such file or directory" error message. With this update, the ppc64-diag package specifies the location of the message_catalog directory correctly, which prevents the described error from occurring.

BZ#1131501

Prior to this update, the /var/lock/subsys/rtas_errd file was incorrectly labeled for SELinux as "system_u:object_r:var_lock_t:s0". This update corrects the SELinux label to "system_u:object_r:rtas_errd_var_lock_t:s0".

Users of ppc64-diag are advised to upgrade to these updated packages, which correct these issues and add these enhancements.

7.166. ppp

7.166.1. RHBA-2015:0685 — ppp bug fix and enhancement update

Updated ppp packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The ppp packages contain the Point-to-Point Protocol (PPP) daemon and documentation for PPP support. The PPP protocol provides a method for transmitting datagrams over serial point-to-point links. PPP is usually used to dial in to an Internet Service Provider (ISP) or other organization over a modem and phone line.

Bug Fixes

BZ#906912

Previously, when the radius client configuration file contained an option not recognized by the PPP radius plug-in, an error was reported. To fix this bug, the parser for the configuration file has been amended to skip unrecognized options. Now, unknown options are skipped without reporting errors.

BZ#922769

Prior to this update, the ppp package incorrectly required the logrotate package. Consequently, the logrotate package could not be easily uninstalled. To fix this bug, the hard dependency on the logrotate package has been removed, and it is now possible to easily uninstall the logrotate package.

BZ#1197792

Previously, the Point-to-Point Protocol daemon (PPPD) terminated unexpectedly when the pppol2tp plug-in was used, and the PPPD command line contained a dump option. To fix this bug, the initialization of the variable containing textual representation of the file descriptor passed to the pppol2tp plug-in has been corrected. Now, the variable initializes properly, and PPPD no longer crashes in this scenario.

Enhancement

BZ#815128

The ppp package now includes two new plug-ins (pppol2tp.so and openl2tp.so) that allow the use of kernel mode l2tp in dependent packages. As a result, it is now possible to leverage in-kernel pppo-l2tp protocol implementation by xl2tpd and openl2tpd.

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

7.167. procps

7.167.1. RHBA-2015:1407 — procps bug fix and enhancement update

Updated procps packages that fix two bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The procps packages contain a set of system utilities that provide system information. The procps packages include the following utilities: ps, free, skill, pkill, pgrep, snice, tload, top, uptime, vmstat, w, watch, and pwdx.

Bug Fixes

BZ#1163404

Previously, behavior of the libproc library was unreliable when it was loaded with the dlopen() call after the environment was changed with the setenv() call. As a consequence, an invalid memory access error could occur in libproc. With this update, the find_elf_note() function obtains the auxiliary vector values using a different and safer method based on parsing the /proc/self/auxv file, and the described problem no longer occurs.

BZ#1172059

Prior to this update, the stat2proc() function did not process empty files correctly. Consequently, when an empty stat file was processed, the ps utility could terminate unexpectedly with a segmentation fault. Handling of empty stat files has been fixed, and ps no longer crashes in this scenario.

Enhancements

BZ#1120580

This update introduces the new "--system" option to the sysctl utility. This option enables sysctl to process configuration files from a group of system directories.

BZ#993072

The new "-h" option has been added to the "free" utility. The purpose of this option is to show all output fields automatically scaled to the shortest three-digit representation including the unit, making the output conveniently human-readable.

BZ#1123311

The "w" utility now includes the "-i" option to display IP addresses instead of host names in the "FROM" column.

Users of procps are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.168. pulseaudio

7.168.1. RHBA-2015:0655 — pulseaudio bug fix update

Updated pulseaudio packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

PulseAudio is a sound server for Linux and other Unix-like operating systems. It is intended to be an improved drop-in replacement for the Enlightened Sound Daemon (ESOUND).

Bug Fixes

BZ#812444

Previously, the pulseaudio(1) man page did not mention the PulseAudio cookie file. As a consequence, if a user wanted to connect to the audio server but was logged in with a different user and cookie, the connection failed, and it was not clear from the documentation what the user must do. With this update, the man page has been improved, and the necessary steps can be found there.

BZ#1111375

Prior to this update, certain applications that require lower audio latency produced low-quality sound when using the PulseAudio "combine" module. With this update, the "combine" module uses automatically adjusted audio latency instead of fixed high audio latency. As a result, sound quality is no longer affected when using low-latency applications with the "combine" module.

BZ#1110950

Previously, the following warning message was displayed during the booting process when using PulseAudio :

udevd[PID]: GOTO 'pulseaudio_check_usb' has no matching label in: '/lib/udev/rules.d/90-pulseaudio.rules'

The invalid parameter that caused this problem has been removed from PulseAudio udev rules, and the warning message no longer appears.

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

7.169. pyOpenSSL

7.169.1. RHBA-2015:1337 — pyOpenSSL bug fix and enhancement update

Updated pyOpenSSL packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The pyOpenSSL packages provide a high-level wrapper around a subset of the OpenSSL library for the Python programming language.

Upgrade to an upstream version

The pyOpenSSL packages have been upgraded to upstream version 0.13.1, which provides a number of bug fixes and enhancements over the previous version. (BZ#1036853)

Users of pyOpenSSL are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.170. pykickstart

7.170.1. RHBA-2015:1296 — pykickstart bug fix and enhancement update

An updated pykickstart package that fixes one bug and adds two enhancements is now available for Red Hat Enterprise Linux 6.

The pykickstart package contains a Python library for manipulating Kickstart files.

Bug Fix

BZ#995443

Previously, the pykickstart utility did not enforce using both the "--size=" and "--grow=" options at the same time, which was required by anaconda. As a consequence, the installation failed to complete and the following misleading error message was returned:

ERROR : Unable to create new logical volume with no extents

With this update, pykickstart enforces using both "--size=" and "--grow=" at the same time, and, if the installation fails, displays a clear message that the kickstart file needs to be modified.

Enhancements

BZ#1017061

This update fixes a typographical error in an error message returned when using the "autopart" and "part" utilities at the same time.

BZ#1182624

The "clearpart" command now supports the "--cdl" option that instructs anaconda to reformat any Linux Disk Layout Direct Access Storage Devices (LDL DASDs) to the Compatible Disk Layout (CDL) format. This option is only useful on the System z platform.

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

7.171. python

7.171.1. RHSA-2015:1330 — Moderate: python security, bug fix, and enhancement update

Updated python packages that fix multiple security issues, several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

Red Hat Product Security 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 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).

Security Fixes

CVE-2014-1912

It was discovered that the socket.recvfrom_into() function failed to check the size of the supplied buffer. This could lead to a buffer overflow when the function was called with an insufficiently sized buffer.

CVE-2013-1752

It was discovered that multiple Python standard library modules implementing network protocols (such as httplib or smtplib) failed to restrict the sizes of server responses. A malicious server could cause a client using one of the affected modules to consume an excessive amount of memory.

CVE-2014-4650

It was discovered that the CGIHTTPServer module incorrectly handled URL encoded paths. A remote attacker could use this flaw to execute scripts outside of the cgi-bin directory, or disclose the source code of the scripts in the cgi-bin directory.

CVE-2014-7185

An integer overflow flaw was found in the way the buffer() function handled its offset and size arguments. An attacker able to control these arguments could use this flaw to disclose portions of the application memory or cause it to crash.

These updated python packages also include numerous bug fixes and enhancements. Space precludes documenting all of these changes in this advisory. For information on the most significant of these changes, users are directed to the following article on the Red Hat Customer Portal:

https://access.redhat.com/articles/1495363

All python users are advised to upgrade to these updated packages, which contain backported patches to correct these issues and add this enhancement.

7.172. python-nss

7.172.1. RHBA-2015:1324 — python-nss bug fix and enhancement update

Updated python-nss packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The python-nss packages provide bindings for Network Security Services (NSS) that allow Python programs to use the NSS cryptographic libraries for SSL/TLS and PKI certificate management.

Upgrade to an upstream version

The python-nss packages have been upgraded to upstream version 0.16.0, which provides a number of bug fixes and enhancements over the previous version. (BZ#1154776)

Bug Fix

BZ#1154776

Added support for setting trust attributes on a certificate. * Added support for the SSL version range API, information on the SSL cipher suites, and information on the SSL connection.

Users of python-nss are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.173. python-virtinst

7.173.1. RHBA-2015:1372 — python-virtinst bug fix update

An updated python-virtinst package that fixes several bugs is now available for Red Hat Enterprise Linux 6.

The python-virtinst package contains several command-line utilities, including virt-install for building and installing new virtual machines, and virt-clone for cloning existing virtual machines.

Bug Fixes

BZ#1172407

Previously, the virt-manager tool generated an invalid XML code when defining a bridge interface. As a consequence, bridge devices could not be created. With this update, virt-manager generates the correct definition XML and creating bridge devices no longer fails.

BZ#1167998

Prior to this update, input from the user was validated incorrectly by the virt-install utility. Consequently, a non-sparse LVM could not be created and an error message was displayed. This update fixes the input validation and virt-install can now create a non-sparse LVM as expected and an error no longer occurs.

BZ#1167072

Previously, changing the processor type to "copy from host" caused all CPU extensions to be copied manually, even extensions that were not supported for migration. As a consequence, running the "virsh save" command after reboot failed, and an error message was displayed. With this update, when the "--cpu=host" option is specified, the "cpu mode='host-model'" option is used. As a result, unsupported extensions are not no longer manually copied, and the described error no longer occurs.

Users of python-virtinst are advised to upgrade to this updated package, which fixes these bugs.

7.174. qemu-kvm

7.174.1. RHBA-2015:1275 — qemu-kvm bug fix and enhancement update

Updated qemu-kvm packages that fix one bug and add various enhancements are now available for Red Hat Enterprise Linux 6.

KVM (Kernel-based Virtual Machine) is a full virtualization solution for Linux on AMD64 and Intel 64 systems. The qemu-kvm packages provide the user-space component for running virtual machines using KVM.

Bug Fix

BZ#1115340

When a KVM virtual machine (VM) running on a Red Hat Enterprise Linux 6 host was suspended to disk and then restored, the system time on the VM in some cases did not correctly synchronize with the system time on the host. With this update, the kvm-clock utility has been modified to reliably read the system time on the host, and the described problem no longer happens.

Enhancements

BZ#1149120

Support has been added for qemu-kvm trace events during the system shutdown process, which allows users to get detailed diagnostics about systems shutdown requests issued by the "virsh shutdown" command or the virt-manager application. This provides users with enhanced capabilities for debugging KVM guest problems during shutdown.

BZ#1040220

The qemu-img tool now uses the fallocate() system call when the "preallocation=full" option is specified. This makes the preallocation operation significantly faster if "preallocation=full" is used, and thus shortens the time necessary to prepare a new guest.

BZ#1186914

With this update, qemu-kvm supports the "cache=directsync" option in the host file, which enables the use of the directsync cache mode on virtual disks. When "cache=directsync" is used, write operations on the guest are only completed when data is safely present on the disk, which increases data security during file transactions between guests.

Users of qemu-kvm are advised to upgrade to these updated packages, which fix this bug and add these enhancements. After installing this update, shut down all running virtual machines. Once all virtual machines have shut down, start them again for this update to take effect.

7.175. quota

7.175.1. RHBA-2015:1262 — quota bug fix update

Updated quota packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The quota packages contain a suite of system administration tools for monitoring and limiting user and group disk usage on file systems.

Bug Fixes

BZ#1007785

A regression caused incomplete synchronization of the clustered Global File System 2 (GFS2). As as consequence, queries for quota limits over the network timed out. With this update, the algorithm for translating quota values to the network format has been changed to prevent indefinite cycling in the rpc.rquotad server. As a result, a file system with negative quota values can no longer make the remote procedure call quota service unresponsive.

BZ#1009397

Previously, the reported disk usage exceeded the file system capacity because of listing disk usage on a clustered GFS2 file system when a local node was not fully synchronized. Now, disk usage and quotas are printed as signed numbers to reflect the fact that negative fluctuations in disk usage accounting do occur in unsynchronized nodes of clustered file systems. As a result, negative disk usage values are properly reported.

BZ#1024097

Prior to this update, the rpc.quotad server terminated with the "Too many autofs mount points." error when querying for disk quotas over the network to a server that has automounted more than 64 file systems. To fix this bug, the code enumerating automounted file systems has been altered. Now, quota tools suppressing automounted file systems do not impose any limit on their number.

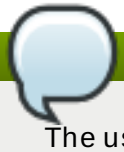
Users of quota are advised to upgrade to these updated packages, which fix these bugs.

7.176. rdma

7.176.1. RHBA-2015:1415 — rdma bug fix and enhancement update

Updated rdma packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

Red Hat Enterprise Linux includes a collection of Infiniband and iWARP utilities, libraries and development packages for writing applications that use Remote Direct Memory Access (RDMA) technology.



Upgrade to an upstream version

The user space libcxgb4 driver has been upgraded to upstream version 1.3.1, which provides a number of bug fixes and enhancements over the previous version. (BZ#1165842)

The user space library infinipath-psm has been upgraded to upstream version 3.3, which provides a number of bug fixes and enhancements over the previous version. (BZ#1138643)

Bug Fixes

BZ#1159331

When shutting down a system with InfiniBand (IB) modules loaded, the system displayed a "Failed to unload ib_addr" error message during the shutdown process. This update corrects the order in which IB modules are unloaded, and the error message no longer appears.

BZ#1151159

Prior to this update, shutting down the nfs-rdma service failed and printed the following message in the console:

Please stop the nfs-rdma service before stopping the rdma service.

The order of nfs-rdma shutdown steps has been corrected, and nfs-rdma now stops correctly.

BZ#1006988

Previously, the mstvpd program failed with a segmentation fault when used. With this update, the underlying code has been fixed, and the problem no longer occurs.

Enhancement

BZ#1186498

The ifup-ib script artificially limited the maximum transmission unit (MTU) amount of IP over InfiniBand (IPoIB) devices running in datagram mode to 2044. This has been fixed, and the new limit now depends on the underlying MTU of the InfiniBand fabric. As a result, IPoIB devices can now have MTU up to 4092 if the InfiniBand fabric MTU is also 4092.

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

7.177. redhat-release-server

7.177.1. RHBA-2015:1260 — redhat-release-server bug fix and enhancement update

An updated redhat-release-server package that fixes several bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

The redhat-release-server package contains the Red Hat Enterprise Linux Server release files.

This updated redhat-release-server package reflects changes made for the release of Red Hat Enterprise Linux 6.7.

Enhancement

BZ#1080012

The redhat-release-server package now includes default product certificates related to Beta, HTB, and GA product IDs. These certificates are consumed by the subscription-manager utility.

Users of Red Hat Enterprise Linux 6 are advised to upgrade to this updated redhat-release-server package.

7.178. redhat-rpm-config

7.178.1. RHBA-2015:1396 — redhat-rpm-config bug fix update

An updated redhat-rpm-config package that fixes several bugs is now available for Red Hat Enterprise Linux 6.

The redhat-rpm-config package is used during the build of RPM packages to apply various default distribution options determined by Red Hat. Also, redhat-rpm-config provides a few Red Hat RPM macro customizations, such as those used during the building of Driver Update packages.

Bug Fixes

BZ#842761

Prior to this update, the find-requires.ksyms script provided by the redhat-rpm-config package could not locate the kernel Application Binary Interface (ABI) reference files provided by the kabi-whitelists package. As a consequence, building an RPM that contained a kernel module (*.ko) resulted in the "KERNEL ABI COMPATIBILITY WARNING" error message, and no compatibility check was performed. With this update, the kernel ABI reference files can be successfully located, and ABI compatibility of kernel object files can now be verified in the described situation.

BZ#1179521

RPM scans files during the build process for dependencies, and if a file is accidentally detected as a script by libmagic, RPM parses the first line for the "#!" string to get the interpreter. Previously, RPM could pick up random data if the "#!" string was not included at the beginning of the file. With this update, the RPM verification process is more thorough, and incorrect requirements are no longer picked up.

BZ#1199983

With this update, the redhat-rpm-config package has been added as a dependency of the rpm-build package. A new RPM virtual provide has been added to the system-rpm-config package, which allows system-rpm-config to be required by rpm-build while still being able to be replaced by a third party package.

Users of redhat-rpm-config are advised to upgrade to this updated package, which fixes these bugs.

7.179. redhat-support-tool

7.179.1. RHBA-2015:1406 — redhat-support-tool and redhat-support-lib-python update

Updated redhat-support-tool and redhat-support-lib-python packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The redhat-support-tool utility facilitates console-based access to Red Hat's subscriber services and gives Red Hat subscribers more venues for accessing the content and services available to them as Red Hat customers. Further, it enables Red Hat customers to integrate and automate their helpdesk services with our subscription services.

Bug Fixes

BZ#1198411

Previously, bugs in the redhat-support-lib-python library caused the "addattachment" command to fail with an error message "TypeError: unhashable type" when files were

uploaded using FTP through an HTTP proxy configured to proxy FTP. As a consequence, attachments could not be sent to the RedHat FTP dropbox if redhat-support-tool was configured to use an HTTP proxy and the "-f" option was used with the "addattachment" command. The underlying redhat-support-lib-python code has been fixed, and the "redhat-support-tool addattachment -f" command now successfully uploads files to the RedHat FTP dropbox in this scenario.

BZ#1146360

Due to bugs in redhat-support-lib-python, the "addattachment" command failed with an error message "unknown URL type" when files were uploaded to the Customer Portal using an HTTP proxy. Consequently, attachments could not be added to cases if redhat-support-tool was configured to use an HTTP proxy. This bug has been fixed, and the "redhat-support-tool addattachment" command now successfully uploads files to the Customer Portal through an HTTP proxy.

BZ#1198616

When retrieving case information from the Customer Portal using the /rs/case Representational State Transfer (REST) endpoint, the case group number was included in the response but not in the case group name. Consequently, when viewing the case details with the "redhat-support-tool getcase" command, the case group number and name were not displayed. With this update, an additional call to the /rs/groups endpoint has been added, and "redhat-support-tool getcase" now displays the case group name along with other case information.

BZ#1104722

Previously, the way redhat-support-tool stored Customer Portal passwords was inconsistent in terms of encoding and decoding. As a consequence, certain passwords could not be decoded correctly. With this update, the method of decoding of the stored Customer Portal passwords has been made consistent with how the passwords were encoded, and the described problem no longer occurs.

Users of redhat-support-tool and redhat-support-lib-python are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.180. resource-agents

7.180.1. RHBA-2015:1280 — resource-agents bug fix and enhancement update

Updated resource-agents packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The resource-agents packages provide the Pacemaker and RGManager service managers with a set of scripts that interface with several services in order to allow operating in a High Availability (HA) environment.

Bug Fixes

BZ#1085109

The lvm.sh agent was unable to accurately detect a tag represented by a cluster node. Consequently, the active logical volume on a cluster node failed when another node rejoined the cluster. Now, lvm.sh properly detects whether tags represent a cluster node. When nodes rejoin the cluster, the volume group no longer fails on other nodes.

BZ#1150702

If the file system used by a MySQL resource became unavailable, the MySQL agent's validation checks prevented the resource from stopping. This bug has been fixed, and MySQL resources are now properly restarted in the described case.

BZ#1151379

The RGManager resource agent failed to recognize that Oracle Database started successfully when notifications about non-critical errors were printed on startup. This update modifies the behavior of RGManager to ignore the non-critical errors, so that the Oracle Database service does not fail in this situation.

BZ#1159805

Floating IPv6 addresses managed by the RGManager ip.sh agent did not send unsolicited advertisement packets when starting. Consequently, when an IP resource failed over, it took about five minutes for the tables to be updated. The packets are now sent, which optimizes the time required before an IP address is recognized as being available.

BZ#1161727

When a node experiences a loss of quorum, the RGManager utility performs an emergency stop of all resources, not just those that are in a started state. Previously, when a separate node split from the cluster and lost quorum, the vg_stop_single() function stripped the Logical Volume Manager (LVM) tags from the Volume Group (VG) if the vg_owner was set. With this update, the LVM agent strips the tags only when the local node performing the stop operation is the owner, and the service now runs as part of the quorate partition even if the service owner's LVM tags have been removed.

BZ#1179412

Due to a regression, some NFS options went missing in the nfsserver after updating, and it was impossible to modify the number of the NFS thread. A patch has been applied, and the number is now modifiable.

BZ#1181187

When monitoring a cluster network interface, the IPaddr2 agent could display an "ERROR: [findif] failed" message even though the IP address and interface were working properly. This update fixes the underlying code, and the IPaddr2 agent consistently reports accurate results during the monitor operation.

BZ#1183148

The MySQL agent failed to work if configured with a user other than 'mysql'. Consequently, MySQL failed to start due to a permission error manifested as a timeout error. A fix has been applied, and MySQL now starts and runs as the configured user.

BZ#1183735

Under certain circumstances, the write test of the is_alive() function did not properly detect and report when a file system failed and was remounted as read-only. This update fixes the bug and in the described scenario, is_alive() now reports the status of the file system correctly.

Enhancements

BZ#1096376

The Pacemaker nfsserver agent now sets the rpc.statd TCPPORT or UDPPORT via configuration options.

BZ#1150655

The nginx resource agent now allows an nginx web server to be managed as a Pacemaker cluster resource. This provides the ability to deploy the nginx web server in a high availability environment.

BZ#1168251

The resource-agents-sap-hana package now provides two Pacemaker resource agents, SAPHanaTopology and SAPHana. These resource agents allow configuration of a Pacemaker cluster to manage a SAP HANA Scale-Up System Replication environment on Red Hat Enterprise Linux.

Users of resource-agents are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.181. rgmanager

7.181.1. RHBA-2015:1402 — rgmanager bug fix update

Updated rgmanager packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The rgmanager packages contain the Red Hat Resource Group Manager, which is used for creating and managing high-availability server applications in the event of system downtime.

Bug Fix

BZ#1151199

Previously, when relocating a service, the rgmanager utility attempted to use all nodes in a domain and if all failed, rgmanager restarted the service locally without checking whether the local node was eligible to run the service and regardless of whether the service had been started. Consequently, under certain circumstances, a service in a restricted domain could be started on a non-member node. With this update, if the service cannot be started on any domain members, the service goes back to a stopped state, and rgmanager no longer attempts to start the service on a local node outside the restricted domain.

Users of rgmanager are advised to upgrade to these updated packages, which fix this bug.

7.182. rhn-client-tools

7.182.1. RHBA-2015:1395 — rhn-client-tools bug fix update

Updated rhn-client-tools packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

Red Hat Network Client Tools provide programs and libraries that allow a system to receive software updates from Red Hat Network.

Bug Fixes

BZ#871028

When the rhnpush command was executed with the --server option, and the sslCACert variable was pointing to a non-existent path, rhnpush failed even when the connection to the server used the http protocol instead of https. With this update, rhnpush searches for CA certificate only when it is necessary, which prevents the described failure from occurring.

BZ#1003790

Previously, the rhn_check command returned an exception when processing a script that contained non-ascii characters. With this update, rhn_check accepts non-ascii characters as expected.

BZ#1036586

When executing the rhnpush command without any options, the command redundantly prompted for user credentials, and afterwards displayed a usage message about missing options. With this update, the command displays available options without asking for credentials.

BZ#1094776

Red Hat Network Client Tools did not calculate the CPU socket information on certain systems properly. With this update, rhn-client-tools parse the /proc/cpuinfo file correctly and thus provide the correct CPU socket information for all systems.

BZ#1147319, BZ#1147322, BZ#1147890, BZ#1147904, BZ#1147916

Several minor bugs have been fixed in various localizations of the Red Hat Network Client Tools GUI.

BZ#1147425

Previously, when running the "firstboot --reconfig" command on the system that was already registered with the Red Hat Subscription Management, the boot procedure failed on the Choose Service page. This bug has been fixed, and the exception no longer occurs on registered systems.

Users of rhn-client-tools are advised to upgrade to these updated packages, which fix these bugs.

7.183. ricci

7.183.1. RHBA-2015:1405 — ricci bug fix and enhancement update

Updated ricci packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The ricci packages contain a daemon and a client for remote configuring and managing of clusters.

Bug Fixes

BZ#1187745

Previously, the luci application server and the ccs cluster configuration command in some cases displayed incorrect information about certain aspects of the cluster, such as the daemon status or specific management tasks. With this update, replies to clients' requests against service modules included with the ricci daemon are composed correctly again. As a result, luci and ccs now provide correct information about the cluster.

BZ#1079032

Previously, using the rgmanager utility to disable guest virtual machines (VMs) forced the guests off after 2 minutes. However, when Microsoft Windows guests download system upgrades, they install them during operating system (OS) shutdown. Consequently, if rgmanager forced the Windows guest off during this process, the guest OS could be damaged or destroyed. This update gives the server more time to shut down, and the guest OS can now safely install updates before the shutdown.

BZ#1156157

Prior to this update, the ricci daemon accepted deprecated and insecure SSLv2 connections, which could lead to security issues. With his update, SSLv2 connections are refused, thus fixing this bug.

BZ#1084991

Once authenticated, the ccs utility previously ignored any attempts to re-authenticate. Consequently, the user attempting to re-authenticate with a password did not get an error message even if they used an incorrect password. With this update, ccs verifies the password even if it is already authenticated by ricci, and if the password is not valid, ccs returns an error.

BZ#1125954

Prior to this update, the ccs utility did not properly ignore the SIGPIPE signal. When piping the output of ccs into another program, a traceback could occur if the other program closed the pipe before the ccs process was resolved. Now, ccs properly ignores SIGPIPE, and ccs no longer issues a traceback in the described situation.

BZ#1126872

Previously, the ccs utility did not properly handle comments in the cluster.conf file if they were located in the services section. As a consequence, tracebacks could occur in ccs when listing services. With this update, ccs ignores any comments in the services or resources sections of cluster.conf instead of trying to parse them, thus fixing this bug.

BZ#1166589

The ccs utility did not prevent multiple syncs or activations from executing in one ccs command. Consequently, it was possible to issue a command using multiple options that caused multiple syncs and activations. This update allows only one sync or activation per command, thus fixing this bug.

Enhancement

BZ#1210679

The cluster schema in the ricci packages, used by the ccs utility for offline validation, has been updated. This update includes new options in resource and fence agents packages, and in the rgmanager utility and fenced cluster daemons.

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

7.184. rng-tools

7.184.1. RHBA-2015:1416 — rng-tools bug fix and enhancement update

Updated rng-tools packages that fix several bugs and add various enhancements are now available

for Red Hat Enterprise Linux 6.

The rng-tools packages contain the random number generator user space utilities, such as the rngd daemon.

Upgrade to an upstream version

The rng-tools packages have been upgraded to upstream version 5, which provides a number of bug fixes and enhancements over the previous version. Notably, this update enables the RDRAND and RDSEED hardware random number generator instructions on supported Intel x86- and Intel 64-based EM64T and AMD64 CPU models. (BZ#833620)

Users of rng-tools are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.185. rpm

7.185.1. RHBA-2015:1452 — rpm bug fix and enhancement update

Updated rpm packages that fix several bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

The RPM Package Manager (RPM) is a command-line driven package management system capable of installing, uninstalling, verifying, querying, and updating software packages.

Bug Fixes

BZ#606239

The output of the %posttrans scriptlet was not correctly displayed to the user, which could lead to important errors being ignored. This update introduces a new API that collects the output from the %posttrans scriptlet. As a result, the yum utility can now access the %posttrans output, and displays it to the user.

BZ#833427

Although the RPM Package Manager does not support packages with files larger than 4 GB, the rpm utility allowed creating source packages where individual files exceeded 4 GB. The installation of such packages then failed with a "Digest mismatch" error. Now, rpm no longer allows the creation of such packages, which in turn prevents the described installation failure.

BZ#1040318

On certain architectures, the value of the "LONGSIZE" tag was displayed incorrectly. This update ensures that on these architectures, the value of "LONGSIZE" is converted to the native byte order correctly, and that it is therefore displayed correctly.

BZ#997774

The behavior of the file mode and directory mode parameters for the %defattr directive was changed in a prior update, which caused building packages that still expected the previous behavior to fail or to experience problems. The directive has been reverted to the previous behavior, and a warning about the potential problems with %defattr has been added to the "rpmbuild" command.

BZ#1139805

If the standard output of the rpm utility was redirected to a file and the file system was full, rpm failed without writing any error messages. Now, rpm prints an error message as a standard error output if the described scenario occurs.

BZ#1076277

The rpm utility was unable to download and install packages the remote locations of which were specified with an IPv6 address and a specific path format. Now, rpm automatically uses the "--globoff" option with IPv6 addresses, which turns off cURL globbing, and allows packages to be properly downloaded and installed in the described scenario.

BZ#921969, BZ#1024517

If a Perl script in a package contained a string declared as a here-document that included the "use" or "require" words, or a multiline string with these words, the package in some cases had incorrect dependencies when it was created using the "rpmbuild" command. Now, the "use" and "require" strings are ignored as keywords in here-documents and multiline strings, which prevents the problem from occurring.

BZ#993868

Previously, build scriptlets using the pipe character ("|") in some cases failed. This update properly sets the default handling of the SIGPIPE signal in build scriptlets, thus fixing the bug.

Enhancements

BZ#760793

The OrderWithRequires feature has been added to the RPM Package Manager, which provides the new OrderWithRequires package tag. If a package specified in OrderWithRequires is present in a package transaction, it is installed before the package with the corresponding OrderWithRequires tag is installed. However, unlike the Requires package tag, OrderWithRequires does not generate additional dependencies, so if the package specified in the tag is not present in the transaction, it is not downloaded.

BZ#1178083

The %power64 macro has been added to the rpm packages. This macro can be used to specify any or all 64-bit PowerPC architectures in RPM spec files by using the "%{power64}" string.

Users of rpm are advised to upgrade to these updated packages, which fix these bugs and add these enhancements. All running applications linked against the RPM library must be restarted for this update to take effect.

7.186. s390utils

7.186.1. RHBA-2015:1341 — s390utils bug fix and enhancement update

Updated s390utils packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The s390utils packages contain a set of user space utilities that should be used together with the zSeries (s390) Linux kernel and device drivers.

Bug Fixes

BZ#1142415

Previously, CPUs could be set online and offline too frequently or not often enough, and, depending on the workload, the default rules in the sysconfig file could lead to an adverse behavior. The default sysconfig file has been updated, and the default rules from the cpluplugd config file now prevent the unwanted behavior from occurring.

BZ#1161726

Prior to this update, the state of zFCP devices was not checked when bringing them online. Consequently, an error occurred for devices that were already online. This update adds an appropriate check, and errors no longer occur in the described situation.

BZ#1186407

Previously, the dasdstat data file with statistics was not seekable. Consequently, the dasdstat tool exited with an error message or reported inconsistent data. With this update, the data file is read without using seeks over the file, and the dasdstat tool prints the correct statistics as expected.

BZ#1223722

Prior to this update, the ziorep tools could not handle device BusIDs "a.b.xxxx" with "a" and "b" being non-zero. As a consequence, the ziorep tools could not parse the ziomon configuration file. All occurrences of device BusIDs in the ziorep tools have been fixed to support a full range of possible values. Now, the ziorep tools can process configuration files that use any valid device BusID.

BZ#1203680

Previously, the Bash syntax for comparison was used by the s390.script, which could lead to errors when a different shell was used. With this update, the correct syntax for value comparison is used, and the s390.sh file is processed correctly by all shells.

Enhancements

BZ#1053824

With this update, the zipl boot loader has been rebased to a later version, which enhances maintainability for Linux initial program load (IPL) code and enables easier inclusion of bug fixes and new features in the boot loader.

BZ#1053828

This update improves the performance of the dasdfmt tool and increases the speed of the Direct Access Storage Device (DASD) formatting process. The kernel internal handling of format requests has been reorganized, and the usage of the Parallel Access Volumes (PAV) feature has been enabled to accelerate format requests.

BZ#1053829

With this update, the verified path mask is shown when listing I/O devices by the lscss tool.

BZ#1148118

This update adds support for Control Unit Initiated Reconfiguration (CUIR), which enables detailed path information for DASD devices to be shown in the lsdasd tool.

BZ#1148126

This update includes switch port attributes in the output of the lsqeth command.

BZ#1148128

This update adds the General Parallel File System (GPFS) as a supported partition type into the fdasd tool. This partition type identifies partitions containing GPFS Network Shared Disks (NSD) used to store GPFS file system information.

BZ#1148744, BZ#1211281, BZ#1211282

The dbinfo.sh tool has been enhanced to allow specifying the directory in which data collection takes place and where the final tar archive is stored. This update also extends the range of information that is collected by including guest networking settings, libvirt, and multipath configurations and logs.

Users of s390utils are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.187. samba

7.187.1. RHBA-2015:1383 — samba bug fix update

Updated samba packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

Samba is an open-source implementation of the Server Message Block (SMB) protocol and the related Common Internet File System (CIFS) protocol, which allow PC-compatible machines to share files, printers, and other information.

Bug Fixes

BZ#1117059

Enumerating groups did not work as expected with ID mapping for Winbind configured. Running the "getent group -s winbind" command displayed no output if Winbind could not retrieve a GID from a group in Active Directory (AD). With this update, "getent group -s winbind" correctly lists the groups in the described situation.

BZ#1138552

Previously, Samba could be consuming a lot of CPU resources every 60 seconds. The mechanism for how the smbd service processes reread the printcap configuration has been modified, and Samba no longer causes these periodical increases in CPU consumption.

BZ#1144916

An attempt to use the smbclient utility to access a CIFS share could fail under certain circumstances, and the smbd service logged the attempt as LOGON_FAILURE even when the user provided the correct password. The problem has been fixed, and accessing a CIFS share using smbclient works as expected.

BZ#1163383

Running the "net ads join -k" command could result in a segmentation fault when the /etc/krb5.keytab file contained an existing keytab entry. This update prevents passing an invalid pointer, which caused the segmentation fault, and "net ads join -k" no longer fails in the described situation.

BZ#1164336

Description for the "access based share enum" option has been added to the sharesec(1) man page.

BZ#1164269, BZ#1165750

After the Samba packages upgrade, accessing a printer could fail with error messages. The user could not connect to a printer or print files. When more than 900 printers were registered, the rpcclient utility failed with an error message. A patch has been applied to fix these problems, and printers can be used as expected after upgrading Samba.

BZ#1192211

Creating a snapshot from a Windows 2008 or Windows 7 client on a share using the shadow_copy2 module could fail when the snapshot was restoring a file that did not yet exist in the directory. The "NT_STATUS_OBJECT_NAME_NOT_FOUND" message appeared after the user clicked the restore button. With this update, restoring a snapshot works as expected in the described situation.

BZ#1194549

When two AD domains, each configured in a separate forest, had a two-way trust established, Winbind retrieved incorrect group information after the user logged in. For example, the "id" utility did not display the correct list of groups the user belonged to. Only the supplementary groups from the user's own domain were listed when the user was a member of groups from both domains. With this update, Samba clears the cache after a successful login to ensure the correct user information is used. Running "id" now lists supplementary groups from both trusted domains in the described situation.

BZ#1195456

Samba did not start when the file system was in read-only mode. With this update, the Samba init scripts no longer require write permissions for certain system files. Samba now runs as expected on read-only systems.

BZ#1201611

When the "winbind use default domain = yes" setting was used in combination with the "force user = AD_user_name" setting in the /etc/samba/smb.conf file, the AD domain user specified in the "force user" attribute could not access the share. With this update, setting "winbind use default domain = yes" no longer prevents the AD domain user from accessing the share in the described situation.

Users of samba are advised to upgrade to these updated packages, which fix these bugs. After installing this update, the smb service will be restarted automatically.

7.188. sapconf

7.188.1. RHBA-2015:1329 — sapconf bug fix and enhancement update

An updated sapconf package that fixes several bugs and adds two enhancements is now available for Red Hat Enterprise Linux 6.

The sapconf package contains a script that checks the basic installation of Red Hat Enterprise Linux and modifies it according to SAP requirements. The script ensures that all necessary packages are installed and that configuration parameters are set correctly to run SAP software.

Bug Fixes

BZ#1158407

Prior to this update, the sapconf package was not updated to reflect the changes made to the profiles of the tuned daemon for SAP NetWeaver. As a consequence, As a consequence, the activation of a tuned profile searched for the deprecated "sap" profile, and therefore failed. With this update, using the sapconf script installs the tuned-profiles-sap package if it is not already installed. In addition, the TUNED_SAP_PROFILE variable has been changed to "sap-netweaver". As a result, sapconf now properly uses the "sap-netweaver" profile, and activating a tuned profile proceeds as expected.

BZ#1168422

Previously, the sapconf script set an incorrect value for the MAX_MAP_COUNT_MIN variable. The value has been changed, and sapconf now matches the recommended value from SAP Red Hat Enterprise Linux 6.x Installation Guide.

BZ#1173861

In the SELinux permissive mode, the parameter with the path to the configuration file was missing. As a consequence, the sapconf script was waiting for the user input, which led to sapconf becoming unresponsive. The underlying source code has been fixed, and sapconf no longer hangs in the aforementioned situation.

Enhancements

BZ#1123917

The sapconf manual page has been edited to contain more accurate information.

BZ#1174321

With this update, the output of the sapconf script contains also the information about the version of sapconf, which is practical to know for SAP installation or updates.

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

7.189. sblim-sfcb

7.189.1. RHBA-2015:1432 — sblim-sfcb bug fix update

Updated sblim-sfcb packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

Small Footprint CIM Broker (sblim-sfcb) is a Common Information Model (CIM) server conforming to the CIM Operations over the HTTP protocol. The SFCB CIM server is robust and resource-efficient, and is therefore particularly-suited for embedded and resource-constrained environments. The sblim-sfcb package supports providers written against the Common Manageability Programming Interface (CMPI).

Bug Fixes

BZ#1102477

Due to incorrect buffer handling in the sblim-sfcb server, the wbemcli CIM client returned an error message when trying to connect to sblim-sfcb over the HTTPS protocol. A patch has been provided to fix this bug, and sblim-sfcb is now reachable over HTTPS without any errors.

BZ#1110106

When a sblim-sfcb server was used in combination with Openwsman and the openwsmand service connected locally to the sblim-sfcb server, a defunct process was left behind. As a consequence, a new process could not be created by the system. With this update, Openwsman defunct processes no longer occur after terminating the connection to the sblim-sfcb server.

BZ#1114798

Due to a memory leak in the sblim-sfcb server, the amount of memory consumed by the sfcbd service process was increased. The underlying source code has been modified to fix this bug, and the sfcbd service process no longer causes an unwanted memory consumption increase.

Users of sblim-sfcb are advised to upgrade to these updated packages, which fix these bugs.

7.190. scap-security-guide

7.190.1. RHBA-2015:1334 — scap-security-guide bug fix and enhancement update

Updated scap-security-guide package that fixes several bugs and adds various enhancements are now available for Red Hat Enterprise Linux 6.

The scap-security-guide package provides the security guidance, baselines, and associated validation mechanisms that use Security Content Automation Protocol (SCAP). SCAP Security Guide contains the necessary data to perform system security compliance scans regarding prescribed security policy requirements; both a written description and an automated test (probe) are included. By automating the testing, SCAP Security Guide provides a convenient and reliable way to verify system compliance on a regular basis.

Bug Fixes

BZ#1133963

The SCAP content for Red Hat Enterprise Linux 6 Server is now shipped also in the datastream output format.

* The SCAP content for Red Hat Enterprise Linux 7 Server has been included in order to enable the possibility to perform remote scans of Red Hat Enterprise Linux 7 Server systems from Red Hat Enterprise Linux 6 systems.

* This update also includes the United States Government Configuration Baseline (USGCB) profile kickstart file for a new installation of USGCB-compliant Red Hat Enterprise Linux 6 Server system. Refer to Red Hat Enterprise Linux 6 Security Guide for further details.

BZ#1183034

Previously, when checking the sysctl kernel parameters configuration, the SCAP content recognized only the settings present in the /etc/sysctl.conf file. With this update, the content has been updated to also recognize the sysctl utility settings from additional configuration files located in the /etc/sysctl.d/ directory.

BZ#1185426

Prior to this update, when performing a validation if the removable media block special devices were configured with the "nodev", "noexec", or "nosuid" options, the content could incorrectly report shared memory (/dev/shm) device as the one missing the required setting. With this update, the corresponding Open Vulnerability and Assessment Language (OVAL) checks have been corrected to verify mount options settings only for removable media block special devices.

BZ#1191409

Due to a bug in the OVAL check validation, if the listening capability of the postfix service was disabled, the system property scan returned a failure even if the postfix package was not installed on the system. This bug has been corrected and the feature of the postfix service is now reported as disabled. Also, the underlying scan result returns "PASS" when the postfix package is not installed on the system.

BZ#1199946

An earlier version of the scap-security-guide package included also an Extensible Configuration Checklist Document Format (XCCDF) profile named "test". Since the purpose of this profile is just to check basic sanity of the corresponding SCAP content and it is not intended to be applied for actual system scan, the "test" profile has now been removed.

Users of scap-security-guide are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

7.191. screen

7.191.1. RHBA-2015:1247 — screen bug fix and enhancement update

Updated screen packages that fix one bug and add one enhancement are now available for Red Hat Enterprise Linux 6.

The "screen" utility allows users to have multiple logins on a single terminal.

Bug Fix

BZ#908221

Previously, starting the "screen" utility in the rxvt-unicode-256color terminal emulator failed with a "$TERM too long" error. This update fixes the underlying code and "screen" starts on this emulator as expected.

Enhancement

BZ#1087517

With this update, the "screen" utility logs both successful and unsuccessful authentication attempts to a text terminal locked by "screen". This provides users with an additional venue of monitoring the operations and security of their system.

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

7.192. seabios

7.192.1. RHEA-2015:1355 — seabios enhancement update

An updated seabios package that adds one enhancement is now available for Red Hat Enterprise Linux 6.

The seabios package contains an open-source legacy BIOS implementation which can be used as a coreboot payload. It implements the standard BIOS calling interfaces that a typical x86 proprietary BIOS implements.

Enhancement

BZ#1131530

The user can now access the boot menu by pressing the ESC key. Previously, the boot menu could only be accessed by pressing the F12 key. However, one some platforms, F12 can be unavailable. For example, systems running the OS X operating system can intercept certain function keys, including F12. With this update, the user can use either ESC or F12 to access the boot menu. Therefore, seabios avoids these potential problems associated with F12.

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

7.193. selinux-policy

7.193.1. RHBA-2015:1375 — selinux-policy bug fix and enhancement update

Updated selinux-policy packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The selinux-policy packages contain the rules that govern how confined processes run on the system.

Bug Fixes

BZ#1198047, BZ#1198057, BZ#1198060, BZ#1198064, BZ#1198071, BZ#1198077, BZ#1198165, BZ#1202935, BZ#1203756, BZ#1207140, BZ#1212729

When the /etc/nsswitch.conf file was modified so that the SSSD service was used for various lookups, certain services were not able to communicate with SSSD due to insufficient SELinux policy rules. With this update, the SELinux policy has been modified to allow the services to work as expected in this situation.

BZ#1198436, BZ#1215632, BZ#1228197, BZ#1228197, BZ#1219317, BZ#1221929

With this update, SELinux policy rules for the glusterd, ctdbd, samba, and nagios services have been fixed to allow the Gluster layer product to work with SELinux properly.

Enhancement

BZ#1153712

When writing SELinux policy rules that allow random services to read or execute general files located, for example, in the /etc/ or /usr/ directories, policy writers had to add additional rules for each service. These updated selinux-policy packages introduce the new "base_ro_file_type" and "base_file_type" SELinux attributes, which policy writers can use to declare global rules against a rule per service.

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

7.194. sendmail

7.194.1. RHBA-2015:1299 — sendmail bug fix update

Updated sendmail packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

Sendmail is a Mail Transport Agent (MTA) used to send mail between machines.

Bug Fixes

BZ#640234

Previously, the sendmail macro MAXHOSTNAMELEN allowed only 63 characters for the host name length. However, in some cases, it was used against the length of a fully-qualified domain name (FQDN), which has a maximum length of 255 characters. Consequently, FQDN resolution did not work correctly in some cases. To fix this bug, MAXHOSTNAMELEN now allows a maximum of 255 characters.

BZ#837007

The sendmail queue runner could previously terminate unexpectedly under certain circumstances. Consequently, sendmail stopped processing the mail queue. This update introduces a fix that prevents the source code from triggering an assertion in the OpenLDAP code when the connection to an LDAP server is lost while making a query. As a result, the assertion no longer causes the queue runner to terminate, and sendmail continues processing the mail queue as expected.

BZ#845821

Under certain circumstances, sendmail previously recorded a very large number of log messages that reported failures to set the close-on-exec flag. The Milter implementation has been modified to perform socket validation before the fnctl() function attempts to set close-on-exec. As a result, fnctl() is no longer called on invalid sockets, and the described log messages no longer occur.

BZ#890227

Prior to this update, the ldap_routing feature did not work as expected. If ldap_routing was used, sendmail reported the "-T<TMPF>" option missing, and the user was required to insert "-T<TMPF>" manually. With this update, the macro for generating configuration for ldap_routing has been fixed, and the user is no longer required to add "-T<TMPF>" manually when using ldap_routing.

BZ#1106852

Previously, the "{client_port}" value could not be used on little-endian machines, for example in mail filters, because it was set incorrectly. This update corrects the "{client_port}" value on little-endian machines.

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

7.195. setroubleshoot

7.195.1. RHBA-2015:1361 — setroubleshoot bug fix update

Updated setroubleshoot packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The setroubleshoot packages contain a set of analysis plug-ins for use with the setroubleshoot utility. Each plug-in has the capacity to analyze SELinux Access Vector Cache (AVC) data, as well as system data, to provide user-friendly reports that describe how to interpret SELinux AVC denial messages.

Bug Fixes

BZ#787139

On Red Hat Enterprise Linux 6, the "sealert -a" command previously only displayed a part of the expected output. This update adds the missing line of code, and "sealert -a" now prints the full extent of its output.

BZ#1098068

Prior to this update, the "sealert -V" command did not properly display the verbose debug message. With this update, the underlying code has been adjusted to ensure that the the verbose form of the debug message is printed, and the described problem no longer occurs.

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

7.196. sg3_utils

7.196.1. RHEA-2015:1365 — sg3_utils enhancement update

Updated sg3_utils packages that add one enhancement are now available for Red Hat Enterprise Linux 6.

The sg3_utils packages provide command-line utilities for devices that use the Small Computer System Interface (SCSI) command sets.

Enhancement

BZ#1051363

With this update, the sg3_utils packages introduce more efficient utilities for copying data between storage devices which benefit from the Small Computer System Interface (SCSI) protocol. To enable this functionality, this update backports the sg_xcopy and sg_copy_results programs to the sg3_utils packages.

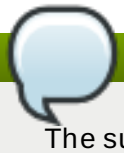
Users of sg3_utils are advised to upgrade to these updated packages, which add this enhancement.

7.197. sos

7.197.1. RHBA-2015:1323 — 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 6.

The sos package contains a set of utilities that gather information from system hardware, logs, and configuration files. The information can then be used for diagnostic purposes and debugging.



Upgrade to an upstream version

The sudo package has been upgraded to upstream version 3.2, which provides a number of bug fixes and enhancements over the previous version. (BZ#1144525, BZ#1190723)

Bug Fixes

BZ#1144525, BZ#1190723

- Increased log size limits.
- Enhanced file archiving and improved sosreport robustness.
- Introduced a number of new plug-ins.
- Implemented the "--profile" option, thus adding profile support for plug-in selection.
- Added the "--verify", "--log-size", and "--all-logs" global plug-in command-line options.
- The time-out limit for commands introduced by this rebase has been extended, providing the crm_report utility enough time to complete.

BZ#912946

The "glusterfsd: no process killed" message could previously be displayed in the standard output stream when generating a report. This update modifies the gluster plug-in to use the built-in callout functions, and the message is no longer displayed in this situation.

BZ#1196717

Prior to this update, if the user defined passwords in the /etc/fstab and /boot/grub/grub.conf files, the sosreport utility included these passwords into the report. Consequently, the report tarball contained the passwords, either in plain text format or hashed, which was considered insecure. With this update, sosreport excludes passwords and other secrets when generating the report. As a result, /etc/fstab and /boot/grub/grub.conf collected in the report tarball do not contain the passwords.

BZ#1203330

Prior to this update, the data collected by the OpenShift sosreport plug-in from certain non-default configuration files could contain sensitive data. The plug-in has been modified to remove any sensitive information from these configuration files. As a result, the OpenShift sosreport plug-in no longer captures sensitive data from the mentioned configuration files.

BZ#1206661

The networking plug-in for the sos utility previously reported an "unhandled exception" error when the NetworkManager tool was disabled. With this update, the status of the nmcli utility is properly checked before the networking plug-in processes its output, which prevents the plug-in from generating the error.

BZ#1206581

Previously, passwords were not removed from some of the files collected by the crm_report utility. Consequently, the data collected by crm_report could contain passwords in plain text format. This update adds the "cluster.crm_scrub" option to sosreport. The option is enabled by default and removes the password information from the crm_report data collected by sosreport. As a result, the data collected by crm_report no longer contains any password information in plain text format.

Enhancement

BZ#1135290

The sosreport plug-in now enables capturing data required to debug Satellite Capsule Server problems.

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

7.198. spice-server

7.198.1. RHBA-2015:1394 — spice-server bug fix update

Updated spice-server packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The Simple Protocol for Independent Computing Environments (SPICE) is a remote display protocol for virtual environments. SPICE users can access a virtualized desktop or server from the local system or any system with network access to the server. SPICE is 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 Hypervisors.

Bug Fixes

BZ#1135372

Prior to this update, when using the "rhel6.0.0" Quick Emulator (QEMU) machine type, the guest could receive invalid drawing commands. Consequently, spice-server terminated unexpectedly. With this update, spice-server detects these invalid drawing commands and ignores them. As a result, spice-server no longer crashes when using the "rhel6.0.0" QEMU machine type.

BZ#1163480

Previously, when using a client with the spice-gtk package version 0.12 or earlier, spice-server did not correctly handle resetting a guest. Consequently, spice-server could terminate unexpectedly with a segmentation fault when resetting a guest. With this update, spice-server properly handles a NULL pointer dereference in the code that handles the spice agent channel, thus avoiding the segmentation fault. As a result, spice-server no longer crashes in this situation.

Users of spice-server are advised to upgrade to these updated packages, which fix these bugs.

7.199. spice-vdagent

7.199.1. RHBA-2015:1392 — spice-vdagent bug fix update

Updated spice-vdagent packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The spice-vdagent packages provide a SPICE agent for Linux guests.

Bug Fixes

BZ#1117764

Previously, when using a SPICE client and the SPICE protocol to connect to a virtual machine, copying and pasting text to and from the client failed for certain applications running in the guest. This update ensures that the spice-vdagent utility properly handles the TIMESTAMP and STRING selection types, and the problem no longer occurs.

BZ#1209550

Prior to this update, SPICE agents in some cases did not properly store the resolution of the guest screen opened by virt viewer. Consequently, the resolution of the guest screen unintentionally changed in certain situations, such as after enabling and disabling a second guest screen. This update ensures that guest screen resolution is stored properly, and thus prevents the described problem.

BZ#1086657

Due to a race condition between the SPICE client and the guest's gnome-settings-daemon, using the SPICE client to re-enable a previously disabled guest display in some cases failed. This update ensures that gnome-settings-daemon no longer unintentionally attempts to enable or disable guest displays, which prevents the problem from occurring.

BZ#1206117

After disabling a guest display using the remote-viewer menu, the disabled display was in some cases immediately re-enabled. This update fixes the underlying code, and disabled guest displays no longer get automatically reactivated.

Users of spice-vdagent are advised to upgrade to these updated packages, which fix these bugs.

7.200. spice-xpi

7.200.1. RHBA-2015:1393 — spice-xpi bug fix update

Updated spice-xpi packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The spice-xpi packages provide the Simple Protocol for Independent Computing Environments (SPICE) extension for Mozilla that allows the SPICE client to be used from a web browser.

Bug Fixes

BZ#1049475

Previously, after enabling a proxy for a SPICE connection opened through the spice-xpi plug-in, the only way the user could unset the proxy was to close or reopen the web page. This update modifies spice-xpi to unset the SPICE_PROXY environment variable when the proxy is unset. As a result, unsetting a proxy for a SPICE connection works as expected.

BZ#1049486

Prior to this update, certain spice-xpi properties were not recorded in the spice-xpi.log file. These properties were only displayed in the /var/log/messages file. With this update, spice-

xpi has been modified to properly log reading or setting the "smartcard", "color-depth", "disable-effects", and "proxy" properties of the spice-xpi browser plug-in. As a result, these events are now visible in spice-xpi.log.

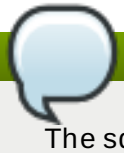
Users of spice-xpi are advised to upgrade to these updated packages, which fix these bugs. After installing the update, Firefox must be restarted for the changes to take effect.

7.201. squid

7.201.1. RHBA-2015:1314 — squid bug fix and enhancement update

Updated squid packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

Squid is a high-performance proxy caching server for web clients, supporting FTP, Gopher, and HTTP data objects.



Upgrade to an upstream version

The squid packages have been upgraded to upstream version 3.1.23, which provides a number of bug fixes and enhancements over the previous version. Among others, this update adds support for the HTTP/1.1 POST and PUT responses with no message body to squid. (BZ#999305)

Bug Fixes

BZ#1202858

During the testing phase, it was discovered that restarting squid caused all files on the system to be deleted. Red Hat has fixed the bug before it could affect any users of squid. As a result, restarting squid does not cause any files on the system to be deleted. This bug was never released neither as part of Red Hat Enterprise Linux, nor as part of any upstream version of the squid packages. For more information about the bug, see the Knowledgebase Solution linked to in the References section.

BZ#1102343

Prior to this update, it was possible to start a new instance of squid while a previous instance was still running. Consequently, the previous instance of squid was running simultaneously with the new instance. This update modifies the squid init script to verify that squid has been terminated before starting a new instance. As a result, the squid init script fails with an error when a new instance is initiated in this scenario, allowing the administrator to properly handle the situation.

BZ#1112842

Under high system load, the squid process sometimes terminated unexpectedly with a segmentation fault during reboot. This update provides better memory handling during reboot, thus fixing this bug.

BZ#1114714

Previously, squid sometimes returned an incorrect tag from the Access Control List (ACL) code when using an external ACL. The bug has been fixed, and squid no longer returns the incorrect ACL tag in this situation.

BZ#1149588

Prior to this update, squid in some cases terminated unexpectedly with the following error message:

xstrdup: tried to dup a NULL pointer!

This update fixes the incorrect error handling that caused this problem. As a result, the described error no longer causes squid to crash.

BZ#1162115

Previously, certain monitoring utilities could not load the Management Information Base (MIB) modules. The obsolete MIB file causing this problem has been updated, and the MIB modules can now be loaded as expected.

BZ#1165618

Previously, it was not possible to log host names. With this update, squid no longer sends malformed DNS PTR queries, and as a result, host names are logged as expected.

BZ#1171967

Prior to this update, squid terminated unexpectedly when it encountered a certain assertion in the squid code. The assertion has been replaced with proper error handling, and squid now handles the described situation gracefully.

BZ#1177413

Previously, squid exceeded the limit of maximum locks set to 65,535 under certain circumstances. Consequently, squid terminated unexpectedly. This update significantly increases the lock limit. The new limit is sufficient to prevent squid from exceeding the maximum limit of locks in usual situations.

Enhancement

BZ#1171947

The squid packages are now built with the "--enable-http-violations" option and allow the user to hide or rewrite HTTP headers.

Users of squid are advised to upgrade to these updated packages, which fix these bugs and add these enhancements. After installing this update, the squid service will be restarted automatically.

7.202. sssd

7.202.1. RHBA-2015:1448 — sssd bug fix and enhancement update

Updated sssd packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The System Security Services Daemon (SSSD) provides a set of daemons to manage access to remote directories and authentication mechanisms.

Note

The sssd packages have been upgraded to upstream version 1.12.4, which provides a number of bug fixes and enhancements over the previous version. (BZ#1168347)

Bug Fixes

BZ#1168363

The "domains=" option for the pam_sss module

BZ#1088402

The UPN (User Principal Name) attribute to identify users and user logins

BZ#1036745

Password expiration warnings for non-password authentication

BZ#1168344

The ID views feature

BZ#1168377

Transferring the user shell attribute from an Active Directory (AD) server to an Identity Management (IdM) client

BZ#1098147

Updating cached entries out-of-band in the background

BZ#1161564

The ad_site option can be used to override the AD site discovered from DNS

BZ#1168357

A new Kerberos plug-in maps Kerberos principals to local SSSD user names

BZ#1168378

Groups for AD trusted users are displayed without logging in

BZ#1171782

The case_sensitive option accepts the "preserve" value.

BZ#1173198

The ldap_access_order option accepts the "ppolicy" value.

BZ#1187642

SSSD can use GPOs on an AD server

BZ#1123291

Applications leveraging identities from SSSD could terminate unexpectedly while invalidating the memory cache using the sss_cache utility. This bug has been fixed, and

using sss_cache is safe.

BZ#1134942

SSSD properly recognizes Windows 2012R2 as an AD server and applies the correct AD-specific performance optimizations.

BZ#1139878

SSSD failed to connect to servers that only allowed authenticated connections to read the rootDSE entry, such as IBM Tivoli LDAP servers. SSSD now retries an authenticated connection after a non-authenticated connection fails while reading rootDSE. As a result, SSSD works as expected with these servers.

BZ#1170910

When the simple_allow_groups and simple_allow_users options contained non-existent and existing entries, SSSD denied access to the existing users or groups. Now, SSSD logs and skips the non-existent entries and correctly handles the existing ones.

BZ#1173738, BZ#1194367

This update fixes bugs that caused SSSD to terminate unexpectedly due to memory errors or when trying to access callback data.

BZ#1135838, BZ#1172865

The sssd-ldap(5) and sssd.conf(5) man pages have been modified.

BZ#1201847

SSSD downloaded an unnecessary amount of data when obtaining information about groups from an AD provider when using POSIX attributes on the server. With this update, SSSD downloads only the information about the group object, not the contents of the group.

BZ#1205382

SSSD did not properly handle the "objectGUID" AD LDAP attribute. Now, SSSD considers "objectGUID" a binary value as expected, and the attribute is stored correctly.

BZ#1215765

If a multi-process program requested the initgroups data immediately after SSSD startup, before the SSSD cache was ready, the NSS responder could incorrectly return an empty group list. With this update, the initgroups requests from a multi-process program with an empty cache work correctly, and the described problem no longer occurs.

BZ#1221358

Setups with "subdomains_provider=none" set for AD domains did not sometimes work as expected. Now, the ldap_idmap_default_domain_sid option value is used for the SSSD main domain, thus fixing the bug. Note that ldap_idmap_default_domain_sid must be set for SSSD to function correctly in this situation.

Enhancement

BZ#1171378

SRV queries now honor the time to live (TTL) values from DNS.

Users of sssd are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.203. strace

7.203.1. RHBA-2015:1308 — strace bug fix and enhancement update

Updated strace packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The strace utility intercepts and records the system calls that are made and received by a running process and prints a record of each system call, its arguments, and its return value to standard error output or a file. It is often used for problem diagnoses, debugging, and for instructional purposes.

Upgrade to an upstream version

The strace packages have been upgraded to upstream version 4.8, which provides a number of bug fixes and enhancements over the previous version. (BZ#919101, BZ#1056828)

Bug Fixes

BZ#919101, BZ#1056828

This update adds several new command-line options: "-y" to print file descriptor paths, "-P" to filter system calls based on the file descriptor paths, and "-I" to control how interactive strace is.

A new command-line utility, strace-log-merge, has been added. This utility can be used to merge timestamped strace output into a single file.

The strace utility now uses optimized interfaces to extract data from the traced process for better performance.

The strace utility now provides improved support for decoding of arguments for various system calls. In addition, a number of new system calls are supported.

BZ#877193

Previously, the strace utility incorrectly handled the return value from the shmat() system call. Consequently, the return value displayed was "?" instead of the address of the attached shared memory segment. This bug has been fixed, and strace now displays the correct return value for the shmat() system calls.

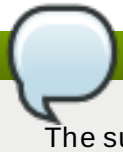
Users of strace are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.204. subscription-manager

7.204.1. RHBA-2015:1345 — subscription-manager and python-rhsm bug fix and enhancement update

Updated subscription-manager, subscription-manager-migration-data, and python-rhsm packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The subscription-manager packages provide programs and libraries to allow users to manage subscriptions and yum repositories from the Red Hat entitlement platform.



Upgrade to an upstream version

The subscription-manager-migration-data package provides certificates for migrating a system from the legacy Red Hat Network Classic (RHN) to Red Hat Subscription Management (RHSM).

The python-rhsm packages provide a library for communicating with the representational state transfer (REST) interface of a Red Hat Unified Entitlement Platform. The Subscription Management tools use this interface to manage system entitlements, certificates, and access to content.

The subscription-manager packages have been upgraded to upstream version 1.14.10, which provides numerous bug fixes and enhancements over the previous version.

The subscription-manager-migration-data package has been upgraded to upstream version 2.0.22, which provides a number of bug fixes and enhancements over the previous version.

The python-rhsm packages have been upgraded to upstream version 1.14.3, which provides a number of bug fixes and enhancements over the previous version. (BZ#1195369)

Bug Fixes

BZ#1159163

Previously, the "yum update --disablerepo" command removed a product certificate. As a consequence, the product was no longer installed on the client and it was impossible to retrieve the content. This bug has been fixed, certificates are no longer removed when the "--disablerepo" option is used, and repositories can now be enabled or disabled as expected.

BZ#1123014

When the .pem certificate file failed to be located, an exit status of 1 was always returned. As a consequence, an error was indicated also in case no products were installed on the system. With this update, when no products are installed and the "--auto-attach" option is used for registering a system, the message "No products installed" is returned to inform the user that there is no need to attach any subscriptions and the system status is "Current" (green). Also, a zero return code indicates that the registration was successful.

BZ#1223860

When configuration options in camelCase are removed from the /etc/rhsm/rhsm.conf file and then restored with the "subscription-manager config" command, they are restored in lowercase. For example, the "subscription-manager config --rhsmcertd.autoattachinterval" command fails to restore the "autoAttachInterval" option in camelCase and, as a consequence, the entry is ignored by the rhsmcertd daemon. However, an existing value can be successfully changed by using such a command. With this update, the

"subscription-manager config --remove" command no longer deletes the option from the configuration file but restores its default value instead. As a result, the described problem occurs only when configuration options are manually deleted from /etc/rhsm/rhsm.conf and not reset with the "--remove" option, which is recommended.

Enhancements

BZ#825089

Subscription Manager now includes certificates and maps for Advanced Mission Critical Update Support (AUS). This enables migration from RHN Classic to RHSM for AUS subscriptions.

BZ#1154375

The rhn-migrate-classic-to-rhsm tool now supports Activation Keys when registering to RHSM. This simplifies automated migration.

BZ#1180273

The rhn-migrate-classic-to-rhsm tool no longer requires RHN Classic credentials if the new "--keep" option is used. This functionality can help simplify automated migration.

Users of subscription-manager, subscription-manager-migration-data, and python-rhsm are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.205. subversion

7.205.1. RHBA-2015:1388 — subversion bug fix update

Updated subversion packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

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.

Bug Fixes

BZ#922718

Previously, properties were lost when merging new files from a foreign repository in Subversion. The underlying source code has been patched to fix this bug, and newly added files retain their properties after a foreign repository merge, as expected.

BZ#1039085

Prior to this update, enabling memcached caching with a Subversion server on Red Hat Enterprise Linux led to excessive socket use, which had a detrimental performance impact. This bug has been fixed, and server performance no longer suffers in this configuration.

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

7.206. sudo

7.206.1. RHSA-2015:1409 — Moderate: sudo security, bug fix, and enhancement update

Updated sudo packages that fix one security issue, three bugs, and add one enhancement are now available for Red Hat Enterprise Linux 6.

Red Hat Product Security 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 sudo packages contain the sudo utility which allows system administrators to provide certain users with the permission to execute privileged commands, which are used for system management purposes, without having to log in as root.

Security Fix

CVE-2014-9680

It was discovered that sudo did not perform any checks of the TZ environment variable value. If sudo was configured to preserve the TZ environment variable, a local user with privileges to execute commands via sudo could possibly use this flaw to achieve system state changes not permitted by the configured commands.

Note: The default sudoers configuration in Red Hat Enterprise Linux removes the TZ variable from the environment in which commands run by sudo are executed.

Bug Fixes

BZ#1094548

Previously, the sudo utility child processes could sometimes become unresponsive because they ignored the SIGPIPE signal. With this update, SIGPIPE handler is properly restored in the function that reads passwords from the user, and the child processes no longer ignore SIGPIPE. As a result, sudo child processes do not hang in this situation.

BZ#1138581

Prior to this update, the order in which sudo rules were processed did not honor the user-defined sudoOrder attribute. Consequently, sudo rules were processed in an undefined order even when the user defined the order in sudoOrder. The implementation of SSSD support in sudo has been modified to sort the rules according to the sudoOrder value, and sudo rules are now sorted in the order defined by the user in sudoOrder.

BZ#1147498

Previously, sudo became unresponsive after the user issued a command when a sudoers source was mentioned multiple times in the /etc/nsswitch.conf file. The problem occurred when nsswitch.conf contained, for example, the "sudoers: files sss sss" entry. The sudoers source processing code has been fixed to correctly handle multiple instances of the same sudoers source. As a result, sudo no longer hangs when a sudoers source is mentioned multiple times in /etc/nsswitch.conf.

Enhancement

BZ#1106433

The sudo utility now supports I/O logs compressed using the zlib library. With this update, sudo can generate zlib compressed I/O logs and also process zlib compressed I/O logs generated by other versions of sudo with zlib support.

All sudo users are advised to upgrade to these updated packages, which contain backported patches to correct these issues and add this enhancement.

7.207. system-config-kickstart

7.207.1. RHBA-2015:1356 — system-config-kickstart bug fix update

An updated system-config-kickstart package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The system-config-kickstart package contains Kickstart Configurator, a graphical tool for creating kickstart files.

Bug Fix

BZ#1022372

Previously, system-config-kickstart tried to display the user manual by executing /usr/bin/htmlview even though this program did not exist, and the underlying code did not handle this situation properly. Consequently, system-config-kickstart terminated. With this update, the user manual, which was in fact outdated and not translated like the rest of the user interface, has been removed from the system-config-kickstart package, and the corresponding menu item has also been removed from the user interface. As a result, system-config-kickstart no longer terminates unexpectedly.

Users of system-config-kickstart are advised to upgrade to this updated package, which fixes this bug.

7.208. system-config-printer

7.208.1. RHBA-2015:0224 — system-config-printer bug fix update

Updated system-config-printer packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The system-config-printer packages contain a print queue configuration tool with a graphical user interface.

Bug Fixes

BZ#854937

Documentation for the pycups library, a part of the system-config-printer packages, was erroneous. The word "as" was missing from some lines and consequently, the code would produce an error when run if the "as" keyword was missing. "As" was added at relevant places to fix this bug. As a result, the documentation text is now correct and complete.

BZ#1063224

Due to erroneous code in the python-cups bindings for libcups, system-config-printer terminated unexpectedly with a segmentation fault when handling UTF-8 characters in certain fields. Now, the execution of system-config-printer no longer results in a segmentation fault.

Users of system-config-printer are advised to upgrade to these updated packages, which fix these bugs.

7.209. system-config-users

7.209.1. RHBA-2015:1433 — system-config-users bug fix update

An updated system-config-users package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The system-config-users package provides a graphical utility for administrating users and groups.

Bug Fix

BZ#981910

When the "INACTIVE" parameter was set in the /etc/default/useradd file, using the system-config-users utility to create or edit a user caused the user to be automatically expired. With this update, setting "INACTIVE" in /etc/default/useradd no longer gives users created or edited in system-config-users an incorrect expiration date, and thus no longer causes them to become unusable.

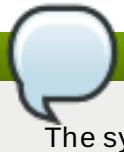
Users of system-config-users are advised to upgrade to this updated package, which fixes this bug.

7.210. systemtap

7.210.1. RHBA-2015:1333 — systemtap bug fix and enhancement update

Updated systemtap packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

SystemTap is an instrumentation system for systems running the Linux kernel, which allows developers to write scripts to collect data on the operation of the system.



Upgrade to an upstream version

The systemtap packages have been upgraded to upstream version 2.7, which provides a number of bug fixes and enhancements over the previous version. (BZ#1158682)

Bug Fixes

BZ#1118352

Previously, some startup-time scripts required the "uprobes.ko" module built, installed, or loaded, but the init script did not identify whether and how to do so. A patch has been applied to fix this bug, and the init script now performs the appropriate operations.

BZ#1147647

Prior to this update, the systemtap scripts caused the "scheduling while atomic" error when running on the Messaging Real-time Grid kernel. To fix this bug, patches have been applied, and the error no longer occurs.

BZ#1195839

The systemtap's "tapset" system call unconditionally included support for the "execveat" system call, even though "execveat" did not exist in Red Hat Enterprise Linux 6 kernels. Consequently, system call probing scripts could fail with a semantic error. With this update, "execveat" is treated conditionally, and the scripts no longer fail in this situation.

Users of systemtap are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.211. sysvinit

7.211.1. RHBA-2015:1362 — sysvinit bug fix update

Updated sysvinit packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The sysvinit packages contain programs that control basic system processes. SysVinit includes the init program, which is the first program started by the Linux kernel when the system boots. The init daemon process is the parent of all processes and continues running until the system is shut down. The sysvinit packages also contain many commonly used utilities, such as reboot, shutdown, poweroff, and sulogin.

Bug Fixes

BZ#760251

If a running binary is replaced, its executable symbolic link in the /proc file system is appended with "(deleted)". Previously, the pidof utility could not handle the suffix. As a consequence, pidof falsely reported that there was no running binary with the original path. With this update, the "(deleted)" suffix is removed when parsing /proc, and pidof works correctly in the described situation.

BZ#883857

Usually, init scripts have the same name as the respective daemons and when the init script looks for the name of the daemon, the PID of the init script that starts the search needs to be excluded. Previously, the pidofproc() function could falsely identify certain processes started by an init script as the daemon of the same name, as the init script could, for example, be running twice. Consequently, pidofproc() failed to return the correct PID of the daemon. With this update, a new "-m" option is available for the pidof utility. The new "-m" option makes it possible to omit any processes that are similar to those explicitly ignored.

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

7.212. tar

7.212.1. RHBA-2015:1285 — tar bug fix update

Updated tar packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The GNU tar program can save multiple files in one archive and restore the files from that archive.

Bug Fixes

BZ#923359

Previously, when the "--verify" or "-W" option was used, the tar utility always exited with a status of 2, and false warning messagess per each archived file were printed. This behavior was a regression introduced in tar-1.23-11.el6. With this update, tar exits with a status of 2 only if there is a real problem with the archived files.

BZ#1034360

Prior to this update, tar interpreted an argument containing an unescaped "[" character and no corresponding "]" character as a pattern-matching string instead of an archive member name, unless the "--no-wildcard" option was used. Consequently, if a user wanted to extract an existing archive member with a path name containing the argument, tar failed to match the argument with the corresponding member, printed an error message, and eventually exited with a non-zero exit status. This problem has been fixed, and tar is now able to extract such a file.

BZ#1056672

Previously, tar did not automatically detect archives compressed by the xz program if the user did not specify the "-J" or "--xz" option on the command line. As a consequence, if the processed archive had the ".xz" extension, tar extracted or listed the contents of the archive but printed an error message and eventually exited with a non-zero exit status. If the archive did not have this extension, tar failed. With this update, the automatic recognition mechanism has been improved. As a result, tar no longer prints an error message in this scenario, and it extracts or lists the contents of such archives correctly regardless of the extension.

BZ#1119312

The tar(1) man page does not list all the available options; however, it now mentions the fact that complete information on using tar is available in the tar Info page, which can be displayed by running the "info tar" command.

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

7.213. tcpdump

7.213.1. RHBA-2015:1294 — tcpdump bug fix and enhancement update

Updated tcpdump packages that fix two bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

The tcpdump packages contain a command-line tool for monitoring network traffic. Tcpdump can capture and display the packet headers on a particular network interface or on all interfaces. Tcpdump can display all of the packet headers, or just the ones that match particular criteria.

Bug Fixes

BZ#972396

Previously, the tcpdump utility was treating the argument for the "-i" option as a number if it contained a numeric prefix and other characters, not as a string. Consequently, packet capturing was not started on a specified interface at all or could get started on a incorrect interface. With this update, the argument for "-i" is treated as a number only if it contains only numerals 0-9; otherwise, the argument is treated as a string. For example, interface names such as "192_1_2" are no longer treated as interface number 192, but as a string. As a result, tcpdump starts correctly on a specified interface even if the interface name contains a numeric prefix.

BZ#1130111

The tcpdump Cisco Discovery Protocol (CDP) dissector previously stopped parsing packet prematurely after encountering Type-Length-Value (TLV) field which had the length of 0 and no data associated with it. Consequently, some CDP packets were not completely dissected. A patch which alters code deciding when to stop parsing the packet has been

applied to fix this bug. Now, zero length data TLVs are allowed, and CDP packets containing such TLVs are parsed correctly.

Enhancements

BZ#1045601

The kernel, glibc, and libpcap utilities now provide APIs to obtain nanosecond resolutions timestamps. The user can thus query which timestamp sources are available ("-J"), set a specific timestamp source ("-j"), and request timestamps with a specified resolution ("--time-stamp-precision").

BZ#1099701

This update adds the new "-P" command-line argument for capturing packets in certain direction, which can ease debugging networking-related problems.

Users of tcpdump are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.214. time

7.214.1. RHBA-2015:0710 — time bug fix update

Updated time packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The GNU time utility monitors the use of system resources by a program. It does so by running the program, collecting information about the resources it uses while running, and displaying the results.

Bug Fix

BZ#703865

Previously, the maximum resident set size (RSS) reported by the GNU time utility was incorrect. To fix this bug, the utility has been amended to reflect the fact that Linux kernel expresses the RSS value in kilobytes, not memory pages. The GNU time utility now reports the maximum RSS value correctly.

Users of time are advised to upgrade to these updated packages, which fix this bug.

7.215. tomcat6

7.215.1. RHBA-2015:1461 — tomcat6 bug fix and enhancement update

Updated tomcat6 packages that fix several bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

Apache Tomcat is a servlet container for the Java Servlet and JavaServer Pages (JSP) technologies.

Bug Fixes

BZ#746842

Previously, in /etc/init.d/tomcat6, the checkpidfile function did not return correct values when the PID file and a matching /proc/${kpid} existed. This caused the status function to use pgrep to look for processes, which showed any other java processes running as the same user. A fix has been applied, and the checkpidfile function now works as expected.

BZ#1022061

Before this update, the tomcat6 init script did not kill the tomcat process if an attempt to stop it was unsuccessful, which prevented tomcat from restarting properly. The init script has been modified to correct this issue.

BZ#1031327

After upgrading from Apache 6.0.20 to a higher version, the file response from the server could be empty in some cases, and empty files without error logs were generated. A patch has been backported, and logs now contain normal responses.

BZ#1042811

Previously, the tomcat6 service restart incorrectly caused duplication in JVM command-line arguments, and the "-Djavax.sql.DataSource.Factory=org.apache.commons.dbcp.BasicDataSourceFact ory" duplicate argument appeared. This has been fixed, and tomcat6 now starts without duplicate JVM arguments.

BZ#1054817

After updating tomcat6-admin-webapps, the "/var/lib/tomcat6/webapps/manager/WEB-INF/web.xml" file was overwritten with a file from the new RPM without notifying the user. This destroyed custom changes made to the file, such as additional roles. The file has been marked as %config in the RPM .spec file. Now, the original file is retained, and the file from RPM is installed as "/var/lib/tomcat6/webapps/manager/WEB-INF/web.xml.rpmnew".

BZ#1128396

Requests using chunked transfer encoding generated a "NullPointerException" in the parseHeader() function of ChunkedInputFilter.java when the last chunk was processed. Consequently, HTTP connection was aborted by tomcat. The underlying code has been amended, and HTTP connection is no longer lost in this situation.

BZ#1183252

Previously, processing a large file, over 1.8 MB in size, by tomcat could lead to an "IOException", and the file was not processed completely. A patch has been applied, and tomcat now processes such files without problems.

BZ#1202759

After upgrading from tomcat6-6.0.24-83 to tomcat6-6.0.24-84, it was not possible to install the IPA server with tomcat6-6.0.24-84, and the "Failed to restart the certificate server" message was displayed. A fix has been applied, and the IPA server can now be installed successfully in this situation.

Enhancements

BZ#844307, BZ#857356

Tomcat 6 can now be installed without a GUI. The dependency on redhat-lsb has been removed, and it is now possible to install Tomcat 6 with a reduced number of installed components without a GUI.

BZ#1068689

Tomcat log file rotation can now be disabled. By default, Tomcat log files are rotated on the first write operation which occurs after midnight, and given the file name {prefix}{date}{suffix}, where the format for date is YYYY-MM-DD. To allow Tomcat log file rotation to be disabled, the parameter "rotatable" has been added. If this parameter is set to "false", the log file is not rotated and the file name is {prefix}{suffix}. The default value is "true".

Users of tomcat6 are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.216. tomcatjss

7.216.1. RHBA-2015:1316 — tomcatjss bug fix and enhancement update

An updated tomcatjss package that fixes one bug and adds one enhancement is now available for Red Hat Enterprise Linux 6.

The tomcatjss package provides a Java Secure Socket Extension (JSSE) implementation using Java Security Services (JSS) for Tomcat, an open source web server and Java servlet container.

Bug Fix

BZ#1190911

Previously, the init() function in tomcatjss looked for the clientauth attribute which was not present. As a consequence, Tomcat returned NullPointerException in init() on startup, and in addition, some properties, such as enableOSCP and properties for enabling certain SSL ciphers, were not called. A patch has been applied to fix this problem. As a result, NullPointerException no longer occurs in the described situation, and the mentioned properties are called as expected.

Enhancement

BZ#1167471

The Tomcat service has been updated to support the Transport Layer Security cryptographic protocol version 1.1 (TLSv1.1) and the Transport Layer Security cryptographic protocol version 1.2 (TLSv1.2) using JSS.

Users of tomcatjss are advised to upgrade to this updated package, which fixes this bug and adds this enhancement.

7.217. tree

7.217.1. RHBA-2015:0049 — tree bug fix update

Updated tree packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The tree package contains the tree utility that recursively displays the contents of directories in a tree-like format. Tree is basically a UNIX port of the DOS tree utility.

Bug Fix

BZ#1110559

Previously, buffer overflows could occur in the uidtoname() and gidtoname() functions of the tree utility. As a consequence, using the "tree" command in some cases failed and the following error message was displayed to the user:

```
*** buffer overflow detected ***: tree terminated
```

An upstream patch has been backported to fix the problem, and the tree utility now lists files as expected.

Users of tree are advised to upgrade to these updated packages, which fix this bug.

7.218. tuna

7.218.1. RHBA-2015:1261 — tuna bug fix update

An updated tuna package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The tuna package provides an interface for changing both scheduler and IRQ tunables at whole-CPU, per-thread, or per-IRQ levels. Tuna allows CPUs to be isolated for use by a specific application and threads and interrupts to be moved to a CPU simply by dragging and dropping them.

Bug Fix

BZ#914366

In Red Hat Enterprise 6.5, the oscilloscope utility was generated successfully, but MRG Realtime was unable to install it. With this update, a specific version of tuna is no longer required, and oscilloscope is thus now installed as expected.

Users of tuna are advised to upgrade to this updated package, which fixes this bug.

7.219. tuned

7.219.1. RHBA-2015:1376 — tuned bug fix update

Updated tuned packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The tuned packages contain a daemon that tunes system settings dynamically. It does so by monitoring the usage of several system components periodically.

Bug Fixes

BZ#1129936

Previously, the tuned service did not support direct-access storage devices (DASDs). As a consequence, DASDs were ignored by tuned and as a result were not configured. This update adds support for DASDs to tuned, and DASDs are now properly configured.

BZ#1036049

On Red Hat Enterprise Linux 6, the /etc/sysctl.conf file is the default configuration file for the sysctl tool settings and overrides can be specified in the /etc/sysctl.d/ directory. The tuned service previously handled the settings the opposite way, which is common in certain distributions. Consequently, the configuration specified in /etc/sysctl.d/ could be overridden

by /etc/sysctl.conf. The way tuned handles /etc/sysctl.conf and /etc/sysctl.d/ has been reversed to match the Red Hat Enterprise Linux 6 logic. As a result, /etc/sysctl.conf is now processed first and can be overridden by settings in /etc/sysctl.d/.

BZ#1159963

Prior to this update, the tuned service did not support Xen Virtual Storage Devices (XVDs). Consequently, XVDs were ignored by tuned and were not configured. Support for XVDs has been added to tuned, and XVDs are now properly configured.

BZ#1174253

Previously, the value of the vm.max_map_count sysctl settings was set too low (1,000,000) in the sap-netweaver tuned profile, which could affect performance. With this update, vm.max_map_count is set to 2,000,000, which is a value recommended by SAP documentation.

BZ#1017366

Previously, certain files from the tuned packages could be incorrectly considered to differ from the RPM database. As a consequence, RPM verification performed by running the "rpm -V tuned" command could fail and it could be indicated that the files were changed despite not being touched by the user. This update excludes several attributes, such as size, md5sum, and mtime, from the verification of the files, and RPM verification no longer fails.

BZ#1064062

Due to a typographical error in the latency-performance profile in the SYSCTL_POST variable, the /etc/sysctl.d/* files were not processed by the tuned service. This update fixes the typographical error, and the /etc/sysctl.d/* files are now correctly processed by tuned.

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

7.220. udev

7.220.1. RHBA-2015:1382 — udev bug fix update

Updated udev packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

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. The udev packages replace the devfs package and provides better hot-plug functionality.

Bug Fixes

BZ#1164960

An earlier update was made to increase the amount of udev workers when some workers were stuck during network module loading, but an incorrect semaphore counter was used. As a consequence, the amount of workers was not increased, and if all workers were busy, timeouts could occur and some events were not correctly processed. With this update, the correct semaphore counter is used, and the amount of available workers now increases as expected.

BZ#1130438

The udev tool did not run the ata_id helper for ATA/ATAPI devices (SPC-3 or later) using the SCSI subsystem. Consequently, those devices, mostly DVD and CD drives, had no ID_SERIAL entry in the udev database and therefore no symbolic link in the /dev/disk/by-id/ directory. With this update, udev calls the ata_id helper on those devices, and the symbolic link in /dev/disk/by-id/ is now present as expected.

BZ#907687

The information displayed for SAS drives in the /dev/disk/by-path/ directory was not a "path" reference, but an "id" reference. Consequently, the symbolic link for SAS drives in /dev/disk/by-path/ changed if the "id" of a component changed. The original scheme uses the disk's SAS address and LUN, and the new scheme introduced by this update uses the SAS address of the nearest expander (if available) and the PHY ID number of the connection. For compatibility reasons, the old symbolic link still exists and a new ID_SAS_PATH environment variable determines a new symbolic link.

BZ#1084513

The udev rules that load a kernel module for a device worked only if the device did not have a driver already, and some modules were not loaded despite being needed. Now, the udev rule no longer checks for the driver.

BZ#1140336

Previously, udev was extended to set the firmware timeout from 60 seconds to 10 minutes to prevent firmware loading timeouts. However, in the early boot phase, the file that is supposed to set this timeout is not present yet. Consequently, an error message was displayed, informing that the /sys/class/firmware timeout file does not exist. Now, udev no longer displays an error message in the described situation.

BZ#1018171

If udev processed the uevent queue for a device that was already removed, the internal handling failed to process an already removed device. Consequently, some symbolic links were not removed for these devices. Now, udev no longer relies on the existence of a device when dealing with the backlog of the uevent queue, and all symbolic links are removed as expected.

BZ#876535

If "udevlog" is specified on the kernel command line to debug udev, all udev logs are stored in the /dev/.udev/udev.log file. Running a system with the udev debug log turned on and using "udevlog" on the kernel command line for an extended period of time could cause /dev/.udev/udev.log to become very large and the devtmpfs mounted on /dev to become full. Consequently, if /dev became full, no new symbolic links and device nodes could be included. With this update, start_udev contains a verbose warning message describing the possibility.

BZ#794561

The ata_id helper of udev did not swap all bytes of the firmware revision information. As a consequence, the firmware revision information of ATA disks stored in the udev database had its last two digits swapped. The ata_id helper has been modified to also swap the last two characters of the firmware revision, and the firmware revision information of ATA disks is now correct.

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

7.221. udisks

7.221.1. RHBA-2015:1336 — udisks bug fix and enhancement update

Updated udisks packages that fix one bug and add two enhancements are now available for Red Hat Enterprise Linux 6.

The udisks packages provide a daemon, D-Bus API, and command-line tools for managing disks and storage devices.

Bug Fix

BZ#1121742

Prior to this update, an external storage device could be unmounted forcefully when a device entered the DM_SUSPENDED=1 state for a moment while performing a set of changes during the cleanup procedure. To fix this bug, an exception for ignoring such a device in the cleanup procedure has been added to the UDisks daemon. As a result, DeviceMapper devices are no longer unmounted forcefully in the described situation.

Enhancements

BZ#673102

With this update, additional mount points and a list of allowed mount options can be specified by means of udev rules. Flexibility of the udev rules format enables the system administrator to write custom rules to enforce or limit specific mount options for a specific set of devices. For example, USB drives can be limited to be always mounted as read-only.

BZ#681875

This update enables the user to configure the udisks tool to enforce the "noexec" global option on all unprivileged users mount points. On desktop systems, the "noexec" option can protect users from mistakenly running certain applications.

Users of udisks are advised to upgrade to these updated packages, which fix this bug and add these enhancements.

7.222. usbredir

7.222.1. RHBA-2015:1381 — usbredir bug fix update

Updated usbredir packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The usbredir packages provide a network protocol for sending USB device traffic over a network connection and a number of libraries to help implement support for this protocol.

Bug Fix

BZ#1085318

Previously, USB redirection over plain Transmission Control Protocol (TCP) sockets with the usbredir packages installed did not work. The USB was not properly redirected in this situation, even though USB redirection over Spice channels worked as expected. This update fixes a bug in the usbredir protocol parser that was causing this problem. As a result, USB redirection over plain TCP sockets now works as expected.

Users of usbredir are advised to upgrade to these updated packages, which fix this bug.

7.223. valgrind

7.223.1. RHBA-2015:1298 — valgrind bug fix update

Updated valgrind packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

Valgrind is an instrumentation framework that is used for debugging memory, detecting memory leaks, and profiling applications.

Bug Fixes

BZ#1196273

Valgrind did not recognize Intel Memory Protection Extensions (MPX) instructions or instructions using the MPX bnd prefix. Consequently, Valgrind terminated programs that used MPX instructions with a SIGKILL signal. Valgrind now recognizes the new MPX instructions and bnd prefixes. All new MPX instructions are currently implemented as no operation instructions, and the bnd prefix is ignored. As a result, programs using MPX instructions or bnd prefixes run under Valgrind as if the MPX was not enabled on the CPU and are no longer terminated.

BZ#1163777

Valgrind was unable to emulate a total LL cache size other than a power of two. Consequently, when detecting CPU caches, Valgrind refused to run the cachegrind tool with a warning message. Now, Valgrind forces down the cache size it emulates to the nearest power of two below the value detected. As a result, cachegrind can be run on systems detected as having a CPU cache size other than a power of two and returns a warning message to indicate the difference between the detected or specified cache size and the emulated cache size.

BZ#1158802

Valgrind assumed that a processor that supported the Advanced Vector Extensions 2 (AVX2) instruction set also always supported the Leading Zeros Count (LZCNT) instruction. This is not always true under QEMU, which can support AVX2 instructions, but not LZCNT. Consequently, Valgrind failed to run under QEMU when AVX2 instructions were enabled. Valgrind has been fixed to be able to run when the AVX2 instruction set is supported but the LZCNT instruction is not, and Valgrind now runs under QEMU as expected.

BZ#1142151

Previously, 32-bit PowerPC (ppc32) binaries that were compiled against the valgrind.h header file to include Valgrind client requests could unexpectedly clobber a register (r0) causing subtle bugs. This problem has been addressed in the client-request code sequence for the ppc32 architecture. Existing ppc32 binaries need to be recompiled against the new valgrind.h header file to fix the bug. Valgrind now also detects the erroneous code sequences in binaries that have not been recompiled and returns a warning message.

BZ#1191404

Valgrind was unable to handle the SIOCETHTOOL ioctl (0x8946), which queries or controls network driver and hardware settings. As a consequence, programs running under Valgrind that use SIOCETHTOOL received a warning message, and arguments were not

tracked by Valgrind. Valgrind now correctly recognizes the SIOCETHTOOL ioctl, and the described problem no longer occurs.

BZ#1191414

Valgrind was unable to recognize the getpriority() and setpriority() system calls on 64-bit PowerPC systems. Consequently, programs running under Valgrind that used the mentioned system calls returned an error message, and arguments to the system call were not tracked. Valgrind has been fixed to recognize the system calls on 64-bit PowerPC systems, and system call arguments are now correctly tracked by Valgrind on all supported architectures.

BZ#1133040

Previously, on the IBM System z architecture, Valgrind did not recognize certain code jumps that depended only on whether the highest bit of a conditional register was fully defined. Consequently, when a program used a combination of the IBM System z LTG + JHE instructions (jump if >= 0) or LTG + JL instructions (jump if < 0), Valgrind reported the following error message: "Conditional jump or move depends on uninitialised value(s)". Valgrind has been fixed to recognize these instruction patterns as jumps that depend only on whether or not the highest bit is set or unset (defined), and the described problem no longer occurs.

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

7.224. vim

7.224.1. RHBA-2015:1310 — vim bug fix and enhancement update

Updated vim packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

Vim (Vi IMproved) is an updated and improved version of the vi editor.

Upgrade to an upstream version

The vim packages have been upgraded to upstream version 7.4, which provides a number of bug fixes and enhancements over the previous version. (BZ#820331, BZ#893239, BZ#1083924, BZ#1112441, BZ#1201834, BZ#1202897, BZ#1204179)

Users of vim are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.225. virt-manager

7.225.1. RHBA-2015:1373 — virt-manager bug fix update

Updated virt-manager packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

Virtual Machine Manager (virt-manager) is a graphical tool for administering virtual machines for KVM, Xen, and QEMU. The virt-manager utility uses the libvirt API and can start, stop, add or remove virtualized devices, connect to a graphical or serial console, and view resource usage statistics for existing virtualized guests on local or remote machines.

Bug Fixes

BZ#1174464

Previously, when using the virt-manager tool to install a guest and checking the "Virtualization tools" box in the "Customize package" menu, virt-manager terminated unexpectedly after the installation was completed and the guest was rebooted. This update fixes the underlying code, and virt-manager no longer crashes in the described scenario.

BZ#1190641

Prior to this update, when using the virt-manager GUI to change the number of CPU threads on the guest, the "Apply" and "Cancel" buttons incorrectly remained disabled. With this update, the signal and callback names in virt-manager have been corrected to properly parse changes to the cpu-thread, and the problem no longer occurs.

Users of virt-manager are advised to upgrade to these updated packages, which fix these bugs.

7.226. virt-viewer

7.226.1. RHBA-2015:1322 — virt-viewer and spice-gtk bug fix and enhancement update

Updated virt-viewer and spice-gtk packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The virt-viewer packages provide Virtual Machine Viewer, which is a lightweight interface for interacting with the graphical display of a virtualized guest.

Upgrade to an upstream version

The spice-gtk packages provide a GIMP Toolkit (GTK+) widget for SPICE (Simple Protocol for Independent Computing Environments) clients. Both Virtual Machine Manager and Virtual Machine Viewer can make use of this widget to access virtual machines using the SPICE protocol.

The virt-viewer packages have been upgraded to upstream version 2.0, which provides a number of bug fixes and enhancements over the previous version. (BZ#1179477)

The spice-gtk packages have been upgraded to upstream version 0.26, which provides a number of bug fixes and enhancements over the previous version. (BZ#1185434)

Bug Fixes

BZ#1205171

When using an emulated smart card on a virtual machine, the smart card was not properly re-initialized after disconnecting and reconnecting the guest. As a consequence, the smart card became unusable. With this update, the smart card state is set properly after reconnecting the guest, and no longer becomes unusable after the operation.

BZ#1032936

The first guest display was re-enabled after a guest reboot even when it was previously disabled on the guest. This update removes the fixed association between the the main guest window and a specific guest display number, which prevents the problem from occurring.

BZ#1111425

In some monitor configurations, after removing a guest display, the display in some cases unintendedly reappeared when the virt-viewer tool was started. The guest now updates its geometry every time a guest display is enabled or disabled, and guest displays now correctly stay removed.

BZ#1021841

When the agent terminated unexpectedly or was disconnected and reconnected again, virt-viewer did not update the information about windows geometry and the guest resolution was not restored accordingly. With this update, the function responsible for updating the displays geometry is called, thus fixing the bug.

BZ#1158086

Using remote-viewer with SSH and the Xming display server caused remote-viewer to terminate unexpectedly. With this update, an assertion no longer triggers in the described circumstances, which prevents the crash from occurring.

BZ#1206216

In multi-display guest setups, the mouse input in some cases affected an incorrect guest display. With this update, displays are properly reordered when their coordinates change, and mouse input reliably affects the appropriate guest display.

Enhancements

BZ#981678, BZ#981677, BZ#806925

The libgovirt and librest packages have been added to this version of Red Hat Enterprise Linux, which allows the remote-viewer tool to connect to the oVirt and Red Hat Enterprise Virtualization virtual machines (VMs). To make it possible to access these VMs, the new ovirt:// URI scheme has also been added to remote-viewer.

BZ#975834

Using the remote-viewer tool to connect to an ovirt:// URI now displays a menu that allows the user to change the CD image inserted in the virtual machine (VM). This makes it possible to change the inserted CD while the VM is running without the need to use Red Hat Enterprise Virtualization or the oVirt portal.

BZ#1129479

It is now possible to configure the position in which guest displays in multi-monitor setups. To do so, edit the ~/.config/virt-viewer/settings file. For more information about this feature, refer to the CONFIGURATION section of the remote-viewer(1) manual page.

Users of virt-viewer and spice-gtk are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.227. virt-who

7.227.1. RHBA-2015:1377 — virt-who bug fix and enhancement update

Updated virt-who package that fixes several bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

The virt-who package provides a service that collects information about virtual guests present in the system and reports them to the subscription manager.

Upgrade to an upstream version

The virt-who package has been upgraded to upstream version 0.12, which provides a number of bug fixes and enhancements over the previous version. (BZ#1195585)

Bug Fixes

BZ#1199397

Previously, virt-who used the value of the "--esx-server" command-line option instead of the "--satellite-server" option value. As a consequence, virt-who attempted to report a host-guest association to the ESX server instead of satellite, and thus failed. With this update, "--satellite-server" works as intended, and virt-who uses the correct server when connecting to Red Hat Satellite.

BZ#1155679

The virt-who service was too slow when reading the association between hosts and guests from VMWare ESX systems. As a consequence, when communicating with large ESX (or vCenter) deployments, it took a lot of time to send updates about virtual guests to the Subscription Asset Manager (SAM) and Red Hat Satellite. With this update, virt-who uses an improved method to obtain host-guest association, which accelerates the aforementioned process.

BZ#1192942

The virt-who service ignored the HTTP proxy configuration in the ESX virtualization back end. As a consequence, virt-who did not use the proxy server when connecting to the ESX server, and the connection could fail. With this update, virt-who uses the http_proxy environment variable in ESX mode, thus fixing this bug.

BZ#1169006

Because certain versions of the VMWare ESX hypervisor do not support the RetrieveProperties method, virt-who failed when obtaining information from the ESX hypervisor. With this update, virt-who no longer uses the RetrieveProperties method and instead works asynchronously, using the WaitForUpdatesEx method. As a result, virt-who is now able to reliable obtain information from the ESX hypervisor.

BZ#1167451

Logging in to a Red Hat Satellite 5 server with virt-who previously failed with an "incomplete format" error. With this update, virt-who uses correct credentials for connecting to Satellite 5 servers, and the login now works.

Enhancements

BZ#1192217

The virt-who service is now capable of filtering which virtualization cluster or clusters it will report. This allows users to automatically filter out clusters that do not contain any Red Hat Enterprise Linux guests, and not to display these redundant clusters.

BZ#1184665

With this update, virt-who allows filtering which hosts are reported to the Subscription Manager. As a result, users can now choose for virt-who not to display hosts with specified parameters, such as hosts that do not run any Red Hat Enterprise Linux guests.

BZ#1173018

The virt-who service can now report the association between hosts and guests when offline, and thus no longer requires connection to the hypervisor to perform this operation. When virt-who cannot be connected to the hypervisor, for instance due to a security policy, users can now obtain information about the host-guest mapping file by using the "virt-who --print" command, which loads the information from the mapping file, and imports it to the Subscription Manager.

BZ#1154877

The support for encrypted passwords has been added to virt-who. Previously, any user with read privileges to the virt-who configuration file was able to read the passwords to external services stored in the configuration file as plain text. This update introduces the virt-who-password utility, which allows encrypting passwords stored in the virt-who configuration file. Note that the root user can still decrypt the encrypted passwords.

Users of virt-who are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

7.228. vsftpd

7.228.1. RHBA-2015:1408 — vsftpd bug fix update

Updated vsftpd packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The vsftpd packages include a Very Secure File Transfer Protocol (FTP) daemon, which is used to serve files over a network.

Bug Fixes

BZ#1063401

Prior to this update, the "local_max_rate" option did not work as expected. As a consequence, the transmission speed was significantly lower. This update extends the types of variables for calculating and accumulating the amount of transferred data and postpones the start of evaluation after the tenth evaluation.

BZ#1092877

Previously, vsftpd server could not handle the use of "pam_exec.so" in the "pam.d" configuration file. Consequently, the vsftpd server considered new processes created by the "pam_exe.so" module to be its own and therefore attempted to catch them. When the processes were caught by "pam_exec.so", the vsftpd server became unresponsive. A patch has been applied to fix this bug, and the vsftpd server no longer hangs in the described situation.

Users of vsftpd are advised to upgrade to these updated packages, which fix these bugs. The vsftpd

daemon must be restarted for this update to take effect.

7.229. wireless-tools

7.229.1. RHBA-2015:1386 — wireless-tools bug fix update

Updated wireless-tools packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The wireless-tools packages contain tools used to manipulate the Wireless Extensions. The Wireless Extension is an interface that allows the user to set Wireless LAN specific parameters and to get statistics for wireless networking equipment.

Bug Fix

BZ#857920

In an environment with a large number of wireless access points, using the wicd connection manager or the network-manager tool to connect to a wireless network previously failed. With this update, the buffer limit of the "iwlist scan" command has been adjusted not to exceed the maximum iwlist buffer amount, which prevents this problem from occurring.

Users of wireless-tools are advised to upgrade to these updated packages, which fix this bug.

7.230. wireshark

7.230.1. RHSA-2015:1460 — Moderate: wireshark security, bug fix, and enhancement update

Updated wireshark packages that fix multiple security issues, several bugs, and add various enhancements are now available for Red Hat Enterprise Linux 6.

Red Hat Product Security 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, previously known as Ethereal, is a network protocol analyzer, which is used to capture and browse the traffic running on a computer network.

Security Fix

CVE-2014-8714, **CVE-2014-8712**, **CVE-2014-8713**, **CVE-2014-8711**, **CVE-2014-8710**, **CVE-2015-0562**, **CVE-2015-0564**, **CVE-2015-2189**, **CVE-2015-2191**

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.

Bug Fixes

BZ#1095065

Previously, the Wireshark tool did not support Advanced Encryption Standard Galois/Counter Mode (AES-GCM) cryptographic algorithm. As a consequence, AES-GCM was not decrypted. Support for AES-GCM has been added to Wireshark, and AES-GCM is now correctly decrypted.

BZ#1121275

Previously, when installing the system using the kickstart method, a dependency on the shadow-utils packages was missing from the wireshark packages, which could cause the installation to fail with a "bad scriptlet" error message. With this update, shadow-utils are listed as required in the wireshark packages spec file, and kickstart installation no longer fails.

BZ#1131203

Prior to this update, the Wireshark tool could not decode types of elliptic curves in Datagram Transport Layer Security (DTLS) Client Hello. Consequently, Wireshark incorrectly displayed elliptic curves types as data. A patch has been applied to address this bug, and Wireshark now decodes elliptic curves types properly.

BZ#1160388

Previously, a dependency on the gtk2 packages was missing from the wireshark packages. As a consequence, the Wireshark tool failed to start under certain circumstances due to an unresolved symbol, "gtk_combo_box_text_new_with_entry", which was added in gtk version 2.24. With this update, a dependency on gtk2 has been added, and Wireshark now always starts as expected.

Enhancements

BZ#1104210

With this update, the Wireshark tool supports process substitution, which feeds the output of a process (or processes) into the standard input of another process using the "<(command_list)" syntax. When using process substitution with large files as input, Wireshark failed to decode such input.

BZ#1146578

Wireshark has been enhanced to enable capturing packets with nanosecond time stamp precision, which allows better analysis of recorded network traffic.

All wireshark users are advised to upgrade to these updated packages, which contain backported patches to correct these issues and add these enhancements. All running instances of Wireshark must be restarted for the update to take effect.

7.231. wpa_supplicant

7.231.1. RHSA-2015:1439 — Low: wpa_supplicant security and enhancement update

An updated wpa_supplicant package that fixes one security issue and adds one enhancement is now available for Red Hat Enterprise Linux 6.

Red Hat Product Security 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 wpa_supplicant package contains an 802.1X Supplicant with support for WEP, WPA, WPA2 (IEEE 802.11i / RSN), and various EAP authentication methods. It implements key negotiation with a WPA Authenticator for client stations and controls the roaming and IEEE 802.11 authentication and association of the WLAN driver.

Security Fix

CVE-2015-4142

An integer underflow flaw, leading to a buffer over-read, was found in the way wpa_supplicant handled WMM Action frames. A specially crafted frame could possibly allow an attacker within Wi-Fi radio range to cause wpa_supplicant to crash.

Enhancement

BZ#1186806

Prior to this update, wpa_supplicant did not provide a way to require the host name to be listed in an X.509 certificate's Common Name or Subject Alternative Name, and only allowed host name suffix or subject substring checks. This update introduces a new configuration directive, 'domain_match', which adds a full host name check.

All wpa_supplicant users are advised to upgrade to this updated package, which contains a backported patch to correct this issue and adds this enhancement. After installing this update, the wpa_supplicant service will be restarted automatically.

7.232. xcb-util

7.232.1. RHBA-2015:1318 — xcb-util bug fix update

Updated xcb-util packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The xcb-util packages provide a number of libraries which utilize libxcb, the core X protocol library, and some of the extension libraries.

Bug Fix

BZ#1167486

The libxcb-icccm.so.1 file was replaced with libxcb-icccm.so.4 in the previous upgrade of the xcb-util packages. Consequently, packages that required the old file could not be installed anymore, or if such packages were installed, xcb-util could not be upgraded. With this update, the libxcb-icccm.so.1 file has been made available again in a new subpackage called compat-xcb-util. As a result, the dependency on libxcb-icccm.so.1 is satisfied.

Users of xcb-util are advised to upgrade to these updated packages, which fix this bug.

7.233. xkeyboard-config

7.233.1. RHBA-2015:1276 — xkeyboard-config bug fix and enhancement update

Updated xkeyboard-config packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The xkeyboard-config packages contain configuration data used by the X keyboard Extension (XKB), which allows selection of keyboard layouts when using a graphical interface.

Bug Fixes

BZ#923160

With the previous upgrade to upstream version 2.11, the /usr/share/X11/xkb/keymap.dir file was removed from the xkeyboard-config packages. Consequently, X11 keyboard configuration stopped working for NX connections. This update includes the missing file again, and as a result, the broken functionality is restored.

BZ#1164507

The previous upgrade to upstream version 2.11 also remapped three keys in the Russian phonetic keyboard layout: the "x" key was mapped to "ha", "h" to "che", and "=" to the soft sign. This change caused problems to users who expected the usual layout of the phonetic keyboard. Now, the layout has been fixed, and these keys are correctly mapped to the soft sign, "ha", and "che" respectively.

Users of xkeyboard-config are advised to upgrade to these updated packages, which fix these bugs.

7.234. xorg-x11-drv-mach64

7.234.1. RHBA-2015:1434 — xorg-x11-drv-mach64 bug fix update

Updated xorg-x11-drv-mach64 packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The xorg-x11-drv-mach64 packages provide the X.Org X11 Mach64 video driver.

Bug Fix

BZ#1182124

Upgrading the xorg-x11-drv-mach64 packages on a Red Hat Enterprise Linux 6 system with the ATI Rage XL VGA video card to Red Hat Enterprise Linux 6.6 introduced a bug. As a consequence, after booting the system in GUI mode, X.Org X11 terminated with a segmentation fault with the Mach64 accelerator. A patch has been applied to address this bug, and X.Org X11 no longer crashes in the described situation.

Users of xorg-x11-drv-mach64 are advised to upgrade to these updated packages, which fix this bug.

7.235. xorg-x11-drv-mga

7.235.1. RHBA-2015:1412 — xorg-x11-drv-mga bug fix update

Updated xorg-x11-drv-mga packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The xorg-x11-drv-mga packages provide a video driver for Matrox G-series chip sets for the X.Org implementation of the X Window System.

Bug Fix

BZ#1177095

Previously, the mga driver used the default color depth of 16 bpp regardless of the configuration. Consequently, it was impossible to run the X server with a custom color depth such as 24 or 32 bpp. With this update, the mga driver honors the configuration properly, and as a result, the desired color depth is used.

Users of xorg-x11-drv-mga are advised to upgrade to these updated packages, which fix this bug.

7.236. xorg-x11-drv-qxl

7.236.1. RHBA-2015:1399 — xorg-x11-drv-qxl bug fix update

Updated xorg-x11-drv-qxl packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The xorg-x11-drv-qxl package provides an X11 video driver for QEMU QXL video accelerator. This driver makes it possible to use Red Hat Enterprise Linux 6 as a guest operating system under the KVM kernel module and the QEMU multiplatform emulator, using the Simple Protocol for Computing Environments (SPICE).

Bug Fixes

BZ#1098647

Previously, the X.org process could become unresponsive after switching to a virtual terminal (VT) and back to a GNOME session with multi-monitor session, meaning 4 monitors opened, or two monitors with a higher resolution, over 1920×1080. A patch has been applied to fix this bug, and X.org no longer hangs in the described scenario.

BZ#1192154

Due to a memory leak in the QXL driver, an X.Org guest could become unresponsive. This update fixes the memory leak, and X.Org no longer crashes.

BZ#1199355

Due to a memory leak in the cursor handling code of the QXL guest driver, the video memory would get saturated and caused a corrupted display when the Anaconda installer was formatting a very large disk (over 2TB). A patch has been applied to prevent cursor data from leaking. As a result, display corruption no longer occurs.

BZ#1151559

Previously, the QXL driver did not correctly handle unexpected drawing commands. As a consequence, the display became unresponsive after entering a space character in the Xfig application. This update fixes the bug in the QXL driver, and Xfig no longer becomes unresponsive in the described situation.

Users of xorg-x11-drv-qxl are advised to upgrade to these updated packages, which fix these bugs.

7.237. xorg-x11-fonts

7.237.1. RHBA-2015:1270 — xorg-x11-fonts bug fix update

Updated xorg-x11-fonts packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The xorg-x11-fonts packages provide X.Org X Window System fonts.

Bug Fix

BZ#1089118

Previously, the Japanese TrueType fonts provided by the ipa-gothic-fonts package were not available through the core X11 font system. This update fixes the xorg-x11-fonts packages, which now correctly provide the required encodings.dir directory listings. As a result, the Japanese TrueType fonts are now available in the core X11 font system as expected.

Users of xorg-x11-fonts are advised to upgrade to these updated packages, which fix this bug.

7.238. xorg-x11-server

7.238.1. RHBA-2015:1445 — xorg-x11-server bug fix and enhancement update

Updated xorg-x11-server packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

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.

Bug Fixes

BZ#963829

The Shift and Caps Lock and Num Lock keys' functionality was reversed when a USB keyboard was unplugged while in Caps Lock or Num Lock mode. Unplugging the keyboard with Caps Lock or Num Lock enabled and later plugging it back in led to incorrect modifier state on the keyboard. Now, the correct modifier state is applied when a keyboard is attached. The discrepancy between the actual and logical status of modifiers no longer occurs.

BZ#1007006

Connecting to a remote machine of different endianness architecture using the X Display Manager Control Protocol (XDMCP) could cause unexpected termination of the X server when the data length in the XkbSetGeometry request was erroneously swapped twice, and an incorrect value was produced. With this update, the data is swapped only once when appropriate, ensuring the use of correct data length. Connecting to remote machines no longer causes X server crashes in this situation.

BZ#1138353

Due to a regression, the "Always" mode of the Xorg server's backing store (-bs) option was not functional, and applications expecting the retention of window content when it was unmapped did not work. The mode has been implemented, and applications that require it now work.

BZ#1161061

The keyboard remained in Caps Lock or Num Lock mode even after the keys were pressed again to change input mode. Now, the Caps Lock and Num Lock functions no longer remain active after pressing the keys to deactivate them.

BZ#1164828

The Xephyr server's 8-bit pseudocolor emulation incorrectly maintained only one colormap for the entire server. When running Xephyr at 8 bpp with multiple screens, only one screen displayed correct colors. Xephyr has been amended to maintain one colormap per screen and now displays correct colors on all screens.

BZ#1171121

The X server package was missing requirements for basic drivers such as vesa, void, or evdev. With this update, installing the X server automatically pulls the basic required drivers as well.

BZ#1177687

The fix for CVE-2014-8092 (RHSA-2014:1983) introduced a type conversion invalid in C++, preventing a C++ application, such as TigerVNC, to be compiled using the X server source files. Now, the header file uses an explicit cast for the type conversion, and C++ applications using X server source files can be compiled.

BZ#1184365

The string format used in error messages was not supported by the X server. When connecting to an unwilling XDMCP server, an error, a backtrace, and termination of the X server occurred instead of displaying an error message. Now, the X server supports the string format, connecting to an unwilling XDMCP server no longer causes a crash, and an error message is displayed prior to exiting cleanly.

BZ#1199591

The X Window System failed to load on reboot when the Xinerama extension and the SELinux module in enforcing mode were enabled. It kept attempting to load the GUI and went on in a loop. Now, the X Window System loads as expected in this situation.

BZ#1208094

Passing a request containing zero height to the XPutImage() function could cause a "division by zero" error in the X server. Now, the X server checks the height value and avoids division by zero. The requests no longer cause errors.

Enhancement

BZ#1049297

The xvfb-run script now accepts the "-a" argument to automatically select an unused display number. Users no longer have to choose one themselves, which was difficult and error-prone when running from automated scripts. The Xvfb server can be used for headless automation setups without the need to specify a display number explicitly.

Users of xorg-x11-server are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

7.239. ypbind

7.239.1. RHBA-2015:1332 — ypbind bug fix and enhancement update

Updated ypbind packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The ypbind packages provide the ypbind daemon to bind NIS clients to an NIS domain. The ypbind daemon must be running on any machines that run NIS client programs.

Bug Fixes

BZ#829487

Previously, the localhost was not treated specifically in the domains list of the ypbind program. Consequently, when the network connection was not established the ypbind did not bind to the ypserv utility on the localhost. With this update, a check for the localhost has been added, and now ypbind works even if the network connection is off.

BZ#842228

Prior to this update, the SIGPIPE signal was not in the proper signal set. Consequently, when a loss of network connectivity occurred, the ypbind utility terminated unexpectedly. Adding SIGPIPE to the proper signal set fixes this bug, and ypbind no longer crashes.

BZ#888778

Previously, the ypbind program's init script did not check for the presence of the ypbind line in the /etc/rpc file. As a consequence, if the ypbind line was not present, ypbind failed to start. This update adds a patch to check for the presence of the ypbind line in /etc/rpc. As a result, ypbind provides a warning message in the log files when its line is missing in /etc/rpc.

Enhancement

BZ#918276

This update adds a configurable option for setting the time interval which is used by the ypbind program to retry rebinding. Previously, ypbind checked for the fastest NIS server every 15 minutes. This in some cases led to intermittent failures when the default timeout interval on a server firewall was set to 10 minutes. The added configurable option allows to set a specific time interval after which ypbind performs a check for the fastest NIS server, and thus avoids the intermittent failures during the rebinding process.

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

7.240. yum

7.240.1. RHBA-2015:1384 — yum bug fix and enhancement update

Updated yum package that fixes several bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

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.

Bug Fixes

BZ#893994

Yum has been updated to detect severity conflicts in the updateinfo.xml file.

BZ#905100

Previously, the "yum grouplist" command terminated unexpectedly with the "ValueError: unknown locale" message when a user-defined locale was specified on the system. With this update, "yum grouplist" has been modified to correctly process user-defined locale files, thus fixing this bug.

BZ#1016148

Under certain circumstances, when attempting to install locally stored packages, yum terminated with the following message:

ValueError: your.rpm has no attribute basepath

This bug has been fixed, and yum now installs local packages as expected.

BZ#1051931

Yum has been modified to properly notify the user if there is not enough space for the installed package in the installation destination. Now, the space required for the package is displayed correctly in MB or KB.

BZ#1076076

Prior to this update, yum did not show the echo output from the %postun RPM scriplet during package removal. This bug has been fixed, and the output is now displayed correctly.

BZ#1144503

Previously, the yum-plugin-downloadonly plug-in returned exit code 1 even when it executed successfully. The functionality of the plug-in has been incorporated into yum as the "--downloadonly" option. The "yum --downloadonly" command now returns the correct exit code on success.

BZ#1171543

The yum-plugin-security plug-in did not show any advisory if the architecture of the updated package changed. This bug has been fixed, and yum-plugin-security now works as expected.

BZ#1200159

Prior to this update, when epoch was defined in the rpm specification file of the kernel package, yum removed the running kernel package after updating. This bug has been fixed, and the running kernel is no longer removed in the described case.

Enhancements

BZ#1154076

The "--exclude" option has been enhanced to exclude the already installed packages.

BZ#1136212

The "yum check" command has been enhanced to execute faster.

BZ#1174612

The "--assumeno" option has been backported to the yum package.

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

7.241. yum-rhn-plugin

7.241.1. RHBA-2015:1390 — yum-rhn-plugin bug fix and enhancement update

Updated yum-rhn-plugin package that fixes two bugs and adds two enhancements is now available for Red Hat Enterprise Linux 6.

The yum-rhn-plugin package allows the Yum package manager to access content from Red Hat Network.

Bug Fixes

BZ#1155129

Previously, provisioning virtual guests on Red Hat Enterprise Linux 6 did not properly cooperate with the Satellite implementation of the koan tool. As a consequence, using the rhn_check program failed if the spacewalk-koan package was installed on the client. With this update, spacewalk-koan has been modified to be compatible with rhn_check, and the described problem no longer occurs.

BZ#1018929

The yum-rhn-plugin package has been updated to support API changes introduced in the previous update of the rhn-client-tools package.

Enhancements

BZ#916597

With this update, the network connection error message has been enhanced to inform about the cause of the error.

BZ#729913

The rhnplugin.conf(5) manual page has been updated to provide the complete description of rhnplugin.conf configuration options.

BZ#1183989

When registering Red Hat Enterprise Linux 6.6 to Red Hat Satellite using an activation key configured to automatically install specific packages upon registration, the installation of these packages in some cases failed. This update fixes the underlying code, and package installations based on the activation key are now performed successfully.

Users of fedfs-utils are advised to upgrade to this updated package, which fixes these bugs and adds this enhancement.

7.242. zsh

7.242.1. RHBA-2015:1273 — zsh bug fix and enhancement update

Updated zsh packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The zsh shell is a command interpreter usable as an interactive login shell and as a shell script command processor. Zsh resembles the ksh shell (the Korn shell), but includes many enhancements. Zsh supports command-line editing, built-in spelling correction, programmable command completion, shell functions (with autoloading), a history mechanism, and more.

Bug Fixes

BZ#1132710

Parameter expansion has been enhanced to provide the ${NAME:OFFSET} and ${NAME:OFFSET:LENGTH} syntaxes for substrings and subarrays present in several other shells.

Numeric expansion with braces has been extended, which allows users to specify a step in the numeric expansion, for example {3..9..2}.

BZ#878324

Prior to this update, when the "jobs -Z" built-in zsh command was invoked, some environment variables were overwritten. An upstream patch has been applied to preserve the environment variables when "jobs -Z" is run, thus fixing this bug.

BZ#1146119

Due to a parser error, the zsh shell previously interpreted variable assignments as other commands, and attempted to execute them when zsh was running in ksh compatibility mode. This update modifies the underlying code to interpret variable assignments as expected in the described situation.

BZ#1131172

Prior to this update, the speed of the pattern matching in the zsh shell decreased when multiple subsequent occurrences of the "*" wildcard symbol were used in a pattern. An upstream patch has been applied on zsh source code to optimize the implementation of pattern matching in zsh with redundant "*" symbols in the pattern. As a result, the speed of pattern matching in zsh is no longer affected by the count of subsequent "*" symbols.

BZ#1103697

An incorrect comment in the /etc/zshenv configuration file caused that the users erroneously expected that the file takes no effect if the zsh shell is started with the "-f" option. The comment in the /etc/zshenv file has been changed to describe the configuration file correctly.

BZ#567215

When processing overly-long input data, the zsh shell terminated unexpectedly because of a stack-based buffer overflow. With this update, arrays of variable sizes are allocated on heap memory instead of stack memory, thus fixing the bug.

BZ#1104021

Prior to this update, the description of emulation mode in the zsh man page was incomplete. With this update, the documentation has been updated to provide users with more information about the command that starts emulation mode.

Users of zsh are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

Appendix A. Revision History

Revision 0.0-1.1 **Mon Jul 20 2015** **Laura Bailey**

Release of the Red Hat Enterprise Linux 6.7 GA Technical Notes.

Revision 0.0-0.2 **Wed Apr 29 2015** **Radek Bíba**

Release of the Red Hat Enterprise Linux 6.7 Beta Technical Notes.