Hewlett Packard Enterprise

HPE 3PAR OS 3.3.1 MU3 Patch 50 Release Notes

Abstract

This release notes document is for 3.3.1 MU3 P50.

Part Number: QL226-10578
Published: January 2019
Edition: 1

Acknowledgements

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Java and Oracle are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Intel®, Itanium®, Pentium®, Intel Inside®, and the Intel Inside logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Purpose

HPE 3PAR OS 3.3.1 MU3 Patch 50 provides enhanced security updates.

IMPORTANT: See the **HPE 3PAR OS and Service Processor Software Update Guide (HPE 3PAR OS 3.3.1 HPE 3PAR Service Processor 5.x)** for instructions on updating your specific software.

Guidance

This is a critical patch.

Prerequisites

- Minimum Service Processor required: SP-5.0.4 + latest SP patch.
- Base OS: 3.3.1 MU3. See the Requires field in the Patch details.

Patch details

Patch ID: P50

Synopsis: Provides enhanced security updates

Date: January 07, 2019, 14:03:55 PST

Description: See the Release Notes for details about this patch

Affected Packages: tpd-basesecuritypatch, tpd-prerevert

Obsoletes: None

Requires: OS-3.3.1.460-MU3

Build Version: 3.3.1.501

Patches Included: None.

Patches Partially Superseded: None.

Patches Obsolete by Combination: None.

Supports Revert: No

Notes:

NOTE:

Hewlett Packard Enterprise recommends installing patches in the same sequence as they are released, unless instructed otherwise.

Modifications

HPE 3PAR OS 3.3.1 MU3 patch 50 addresses the following issues.

```
bind9 (1:9.9.5.dfsg-9+deb8u16) jessie-security; urgency=high
  * Non-maintainer upload by the LTS Team.
  * CVE-2018-5740
    The "deny-answer-aliases" feature in BIND has a flaw which can
    cause named to exit with an assertion failure.

busybox (1:1.22.0-9+deb8u4) jessie-security; urgency=high
```

```
  * Non-maintainer upload the LTS team.
  * Regression update for CVE-2011-5325: It was found that the patch to prevent
    the exploitation of CVE-2011-5325 is too strict in case of cpio archives.
    This update restores the old behavior.

busybox (1:1.22.0-9+deb8u3) jessie-security; urgency=high
  * Non-maintainer upload by the LTS team.
  * Regression update for CVE-2015-9261: Decompressing gzip archives works as
    intended again.

busybox (1:1.22.0-9+deb8u2) jessie-security; urgency=high
  * Non-maintainer upload by the LTS team.
  * Fix CVE-2011-5325:
    A path traversal vulnerability was found in Busybox implementation of tar.
    tar will extract a symlink that points outside of the current working
    directory and then follow that symlink when extracting other files. This
    allows for a directory traversal attack when extracting untrusted tarballs.
  * Fix CVE-2014-9645:
    The add_probe function in modutils/modprobe.c in BusyBox allows local users
    to bypass intended restrictions on loading kernel modules via a / (slash)
    character in a module name, as demonstrated by an "ifconfig /usbserial up"
    command or a "mount -t /snd_pcm none /" command.
  * Fix CVE-2016-2147:
    Integer overflow in the DHCP client (udhcpc) in BusyBox allows remote
    attackers to cause a denial of service (crash) via a malformed
    RFC1035-encoded domain name, which triggers an out-of-bounds heap write.
  * Fix CVE-2016-2148:
    Heap-based buffer overflow in the DHCP client (udhcpc) in BusyBox allows
    remote attackers to have unspecified impact via vectors involving
    OPTION_6RD parsing.
  * Fix CVE-2017-15873:
    The get_next_block function in archival/libarchive/decompress_bunzip2.c in
    BusyBox has an Integer Overflow that may lead to a write access violation.
  * Fix CVE-2017-16544:
    In the add_match function in libbb/lineedit.c in BusyBox, the tab
    autocomplete feature of the shell, used to get a list of filenames in a
    directory, does not sanitize filenames and results in executing any escape
    sequence in the terminal. This could potentially result in code execution,
    arbitrary file writes, or other attacks.
  * Fix CVE-2018-1000517:
    BusyBox project BusyBox wget contains a Buffer Overflow vulnerability in
    Busybox wget that can result in heap buffer overflow. This attack appear to
    be exploitable via network connectivity.
  * CVE-2015-9261:
    Unziping a specially crafted zip file results in a computation of an
    invalid pointer and a crash reading an invalid address.

curl (7.38.0-4+deb8u13) jessie-security; urgency=high
  * Non-maintainer upload by the LTS team.
  * Fix the following security vulnerabilities:
  * CVE-2016-7141:
    When built with NSS and the libnsspem.so library is available at runtime,
    allows remote attacker to hijack the authentication of a TLS connection by
    leveraging reuse of a previously loaded client certificate from file for a
    connection for which no certificate has been set, a different
    vulnerability than CVE-2016-5420.
  * CVE-2016-7167:
    Multiple integer overflows in the (1) curl_escape, (2) curl_easy_escape,
    (3) curl_unescape, and (4) curl_easy_unescape functions in libcurl allow
    attackerrs to have unspecified impact via a string of length 0xffffffff,
    which triggers a heap-based buffer overflow.
  * CVE-2016-9586:
    Curl is vulnerable to a buffer overflow when doing a large floating point
    output in libcurl's implementation of the printf() functions. If there are
    any applications that accept a format string from the outside without
```

```
    necessary input filtering, it could allow remote attacks.
  * CVE-2018-16839:
    Curl is vulnerable to a buffer overrun in the SASL authentication code that
    may lead to denial of service.
  * CVE-2018-16842:
    Curl is vulnerable to a heap-based buffer over-read in the
    tool_msgs.c:voutf() function that may result in information exposure and
    denial of service.

curl (7.38.0-4+deb8u12) jessie-security; urgency=high
  * Fix an NTLM password overflow via integer overflow as per CVE-2018-14618
    https://curl.haxx.se/docs/CVE-2018-14618.html.

dnsmasq (2.72-3+deb8u4) jessie-security; urgency=medium
  * Non-maintainer upload by the LTS team.
  * trust-anchors.conf: include latest DNS trust anchor (KSK-2017).
    (Closes: #907887)

dnsmasq (2.72-3+deb8u3) jessie-security; urgency=medium
  * Non-maintainer upload by the LTS team.
  * Update init service for dns-root-data changes to fix dnsmasq
    startup when dns-root-data is installed. Closes: #860064.

fuse (2.9.3-15+deb8u3) jessie-security; urgency=high
  * Non-maintainer upload by the LTS Team.
  * CVE-2018-10906
    Restriction bypass of the "allow_other" option when SELinux is active

libidn (1.29-1+deb8u3) jessie-security; urgency=high
  * Fix CVE-2017-14062: An integer overflow vulnerability in libidn's Punycode
    handling (an encoding used to convert Unicode characters to ASCII) which
    would have allowed remote attackers to cause a denial of service.
    Patch taken from wheezy, backported by Chris Lamb (Closes: #873903).

libx11 (2:1.6.2-3+deb8u2) jessie-security; urgency=high
  * Non-maintainer upload by the LTS team.
  * Fix CVE-2018-14598, CVE-2018-14599 and CVE-2018-14600:
  * CVE-2018-14599:
    The functions XGetFontPath, XListExtensions, and XListFonts are vulnerable
    to an off-by-one override on malicious server responses.
  * CVE-2018-14600:
    The length value is interpreted as signed char on many systems (depending
    on default signedness of char), which can lead to an out of boundary write
    up to 128 bytes in front of the allocated storage, but limited to NUL
    byte(s).
  * CVE-2018-14598:
    If the server sends a reply in which even the first string would overflow
    the transmitted bytes, list[0] (or flist[0]) will be set to NULL and a
    count of 0 is returned. This may trigger a segmentation fault leading to a
    Denial of Service.

libx11 (2:1.6.2-3+deb8u1) jessie; urgency=medium
  * Insufficient validation of data from the X server can cause out of
    boundary memory read (XGetImage()) or write (XListFonts()).
    Addresses CVE-2016-7942 and CVE-2016-7943.

libxml2 (2.9.1+dfsg1-5+deb8u7) jessie-security; urgency=high
  * Non-maintainer upload by the LTS Team.
  * CVE-2018-14404
    Fix of a NULL pointer dereference which might result in a crash and
    thus in a denial of service.
  * CVE-2018-14567 and CVE-2018-9251
    Approvement in LZMA error handling which prevents an infinite loop.
  * CVE-2017-18258
    Limit available memory to 100MB to avoid exhaustive memory
```

```
    consumption by malicious files.

spice (0.12.5-1+deb8u6) jessie-security; urgency=medium
  * Non-maintainer upload by the LTS Team.
  * CVE-2018-10873:
    A vulnerability was discovered in SPICE before version 0.14.1 where
    the generated code used for demarshalling messages lacked sufficient
    bounds checks. A malicious client or server, after authentication,
    could send specially crafted messages to its peer which would result
    in a crash or, potentially, other impacts.
    .
    Fix: Bail out with an error if the pointer to the start of some
    message data is strictly greater than the pointer to the end of the
    message data.
    .
    See review comments in debian/patches/CVE-2018-10873.patch about
    potential weaknesses of this fix.

tiff (4.0.3-12.3+deb8u7) jessie-security; urgency=high
  * Non-maintainer upload by the LTS Team.
  * CVE-2018-17100
    An int32 overflow can cause a denial of service (application
    crash) or possibly have unspecified other impact via a crafted
    image file
  * CVE-2018-17101
    Out-of-bounds writes can cause a denial of service (application
    crash) or possibly have unspecified other impact via a crafted
    image file
  * CVE-2018-18557
    Out-of-bounds write due to ignoring buffer size can cause a denial
    of service (application crash) or possibly have unspecified other
    impact via a crafted image file

xen (4.4.4lts4-0+deb8u1) jessie-security; urgency=medium
  * Various security fixes:
    - XSA-252 (CVE-2018-7540)
    - XSA-255 (CVE-2018-7541)
    - XSA-260 (CVE-2018-8897)
    - XSA-264 (CVE-2018-12891)
    - XSA-265 (CVE-2018-12893)
    - XSA-268 (CVE-2018-15469)
    - XSA-272 (CVE-2018-15470)
    - XSA-282

xen (4.4.4lts3-0+deb8u1) jessie-security; urgency=medium
  * Various security fixes:
    - XSA-240 (CVE-2017-15595)
    - XSA-242 (CVE-2017-15593)
    - XSA-243 (CVE-2017-15592)
    - XSA-244 (CVE-2017-15594)
    - XSA-246 (CVE-2017-17044)
    - XSA-247 (CVE-2017-17045)
    - XSA-258 (CVE-2018-10472)
    - XSA-262 (CVE-2018-10981)

xen (4.4.4lts2-0+deb8u1) jessie-security; urgency=medium
  * Various security fixes:
    - XSA-231 (CVE-2017-14316)
    - XSA-233 (CVE-2017-14317)
    - XSA-234 (CVE-2017-14319)
    - XSA-236 (CVE-2017-15597)
    - XSA-237 (CVE-2017-15590)
    - XSA-239 (CVE-2017-15589)
    - XSA-241 (CVE-2017-15588)
    - XSA-245 (CVE-2017-17046)
```

```
    - XSA-248 (CVE-2017-17566)
    - XSA-249 (CVE-2017-17563)
    - XSA-250 (CVE-2017-17564)
    - XSA-251 (CVE-2017-17565)
    - XSA-259 (CVE-2018-10471)
    - XSA-261 (CVE-2018-10982)

xen (4.4.4lts1-0+deb8u1) jessie-security; urgency=medium
  * Lastest snapshot of the upstream 4.4 branch (6bf0560), fixing:
    - XSA-206
    - XSA-207 / CVE-2017-14431
    - XSA-178 / CVE-2016-4963

libtirpc (0.2.5-1+deb8u2) jessie-security; urgency=medium
  * Non-maintainer upload by the LTS team.
  * CVE-2018-14622
    Segmentation fault due to pointer becoming NULL.

linux-base (4.5~deb8u1) jessie-security; urgency=medium
  * Rebuild for jessie; no changes required

linux-base (4.5) unstable; urgency=medium
  * Update Danish debconf template translation.
  * Update Brazilian Portuguese debconf templates translation.
  * Update Dutch debconf template translations (Frans Spiesschaert)
    (Closes: #837097)
  * perf: Drop support for versions older than 3.2
  * Use dh with debhelper compat level 9
  * Add bash completion wrapper for perf (Closes: #702482)

linux-base (4.4) unstable; urgency=medium
  * Update debconf template translations:
    - Portuguese (Américo Monteiro) (Closes: #826779)
    - Polish (Lukasz Dulny)
    - Japanese (Victory)
    - Russian (Yuri Kozlov) (Closes: #828772)
    - German (Markus Hiereth)
    - French (Jean-Pierre Giraud) (Closes: #830171)
  * linux-check-removal: Fix substitution of package name in debconf title
  * Update Swedish debconf template translation.
  * Update Czech debconf template translation.

linux-base (4.3) unstable; urgency=medium
  * Add linux-check-removal command for use by package prerm scripts
    - Override lintian warning and error for this unusual debconf usage

linux-base (4.2) unstable; urgency=medium
  * Change source format to 3.0 (native) so that .git directory is excluded
    by default
  * Add manual page for linux-update-symlinks
  * read_kernelimg_conf(): Quietly ignore settings used only by kernel-package
  * debian/rules: Add build-{arch,indep} targets
  * debian/control: Update policy version to 3.9.8; no changes required

linux-base (4.1) unstable; urgency=medium
  * Adjust for migration to git:
    - Add .gitignore files
    - debian/control: Update Vcs-* fields (Closes: #824748)
  * Add image_stem() and read_kernelimg_conf() functions to Perl module
  * Add linux-update-symlinks command for use by package maintainer scripts

linux-base (4.0) unstable; urgency=low
  * Remove obsolete postinst upgrade code and translations
    (Closes: #580435, #660670, #670775, #686211, #686384, #686431, #686445,
     #686459, #686480, #686602, #686610, #686662, #686687, #686704, #686705,
```

```
    #686717, #686720, #686748, #698203)
  * Run version_cmp() unit tests at build time
  * linux-version: Fix sorting of version strings containing -trunk
    (Closes: #761614)
  * perf: Update error message for missing perf executable, to refer to
    linux-perf-<version> for Linux 4.1 onward
  * debian/control: Drop support for pre-multiarch releases
  * debian/control: Update Vcs-* fields to use anonscm.debian.org
  * debian/control: Update policy version to 3.9.6; no changes required

python2.7 (2.7.9-2+deb8u2) jessie-security; urgency=medium
  * Non-maintainer upload by the LTS Security Team.
  * CVE-2018-1000802: fix command injection in shutil module
  * CVE-2017-1000158: fix integer overflow and possible arbitrary code
    execution in the PyString_DecodeEscape function
  * CVE-2018-1060 and CVE-2018-1061: fix REDOS vulnerabilities in poplib
    and difflib modules
```

Verification

The installation of Patch 50 can be verified from an interactive CLI session. Issue the CLI command `showversion -a -b` to verify that Patch 50 is listed:

```
$ showversion -a -b
Release version 3.3.1.460 (MU3)
Patches:  P49,P50

Component Name                   Version
CLI Server                       3.3.1.460 (MU3)
CLI Client                       3.3.1.460
System Manager                   3.3.1.460 (MU3)
Kernel                           3.3.1.460 (MU3)
TPD Kernel Code                  3.3.1.460 (MU3)
CIM Server                       3.3.1.460 (MU3)
WSAPI Server                     3.3.1.460 (MU3)
Console Menu                     3.3.1.460 (MU3)
Event Manager                    3.3.1.460 (MU3)
Internal Test Tools              3.3.1.460 (MU3)
LD Check Tools                   3.3.1.460 (MU3)
Network Controller               3.3.1.460 (MU3)
Node Disk Scrubber               3.3.1.460 (MU3)
PD Scrubber                      3.3.1.460 (MU3)
Per-Node Server                  3.3.1.460 (MU3)
Persistent Repository            3.3.1.460 (MU3)
Powerfail Tools                  3.3.1.460 (MU3)
Preserved Data Tools             3.3.1.460 (MU3)
Process Monitor                  3.3.1.460 (MU3)
Software Updater                 3.3.1.460 (MU3)
TOC Server                       3.3.1.460 (MU3)
VV Check Tools                   3.3.1.460 (MU3)
Upgrade Check Scripts            181001.U016
File Persona                     1.5.3.2-20180914 (P49)
SNMP Agent                       1.13.0
SSH                              7.5p1-5
VASA Provider                    3.0.18 (MU3)
Firmware Database                3.3.1.460 (MU3)
Drive Firmware                   3.3.1.460 (MU3)
UEFI BIOS                        05.04.04 (MU3)
MCU Firmware (OKI)               4.9.01 (MU3)
MCU Firmware (STM)               5.4.00 (MU3)
Cage Firmware (DC1)              4.44 (MU3)
Cage Firmware (DC2)              2.64 (MU3)
Cage Firmware (DC3)              08 (MU3)
Cage Firmware (DC4)              2.64 (MU3)
Cage Firmware (DCN1)             4082 (MU3)
Cage Firmware (DCN2)             4082 (MU3)
Cage Firmware (DCS1)             4082 (MU3)
Cage Firmware (DCS2)             4082 (MU3)
Cage Firmware (DCS5)             2.88 (MU3)
Cage Firmware (DCS6)             2.88 (MU3)
Cage Firmware (DCS7)             4082 (MU3)
Cage Firmware (DCS8)             4082 (MU3)
QLogic QLA4052C HBA Firmware     03.00.01.77 (MU3)
QLogic QLE8242 CNA Firmware      04.15.27
QLogic 260x HBA FC Firmware      174.03.70
QLogic 27xx/268x HBA FC Firmware 174.03.70
QLogic 83xx HBA FCoE Firmware    08.01.05
```

```
QLogic 8300 HBA iSCSI Firmware   05.07.36
Emulex LP11002 HBA Firmware      02.82.x10
Emulex LPe12002 HBA Firmware     02.10.x08
Emulex LPe12004 HBA Firmware     02.10.x08
Emulex LPe16002 HBA Firmware     11.1.220.10
Emulex LPe16004 HBA Firmware     11.1.220.10
3PAR FC044X HBA Firmware         200A8
LSI 9201-16e HBA Firmware        17.11.03
LSI 9205-8e HBA Firmware         17.11.03
LSI 9300-8e HBA Firmware         10.10.03
```

NOTE: When displaying the `showversion` command output from the SP, the CLI Client version is static in the SP code and may differ from the output from any other system.

Websites

General websites

Hewlett Packard Enterprise Information Library

www.hpe.com/info/EIL

Single Point of Connectivity Knowledge (SPOCK) Storage compatibility matrix

www.hpe.com/storage/spock

Storage white papers and analyst reports

www.hpe.com/storage/whitepapers

For additional websites, see **Support and other resources**.

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

  http://www.hpe.com/assistance

- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

  http://www.hpe.com/support/hpesc

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates:

  Hewlett Packard Enterprise Support Center

  www.hpe.com/support/hpesc

  Hewlett Packard Enterprise Support Center: Software downloads

  www.hpe.com/support/downloads

  Software Depot

  www.hpe.com/support/softwaredepot

- To subscribe to eNewsletters and alerts:

  www.hpe.com/support/e-updates

- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

  www.hpe.com/support/AccessToSupportMaterials

IMPORTANT: Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Passport set up with relevant entitlements.

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

http://www.hpe.com/support/selfrepair

Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

Remote support and Proactive Care information

HPE Get Connected

www.hpe.com/services/getconnected

HPE Proactive Care services

www.hpe.com/services/proactivecare

HPE Proactive Care service: Supported products list

www.hpe.com/services/proactivecaresupportedproducts

HPE Proactive Care advanced service: Supported products list

www.hpe.com/services/proactivecareadvancedsupportedproducts

Proactive Care customer information

Proactive Care central

www.hpe.com/services/proactivecarecentral

Proactive Care service activation

www.hpe.com/services/proactivecarecentralgetstarted

Warranty information

To view the warranty information for your product, see the links provided below:

HPE ProLiant and IA-32 Servers and Options

www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise and Cloudline Servers

www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

www.hpe.com/support/Storage-Warranties

HPE Networking Products

www.hpe.com/support/Networking-Warranties

Regulatory information

To view the regulatory information for your product, view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at the Hewlett Packard Enterprise Support Center:

www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional regulatory information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

www.hpe.com/info/reach

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

www.hpe.com/info/ecodata

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

www.hpe.com/info/environment

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (**docsfeedback@hpe.com**). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.