Hewlett Packard Enterprise

HPE 3PAR OS 3.2.2 MU6 Patch 107

Release Notes

Abstract

This release notes document is for Patch 107 and intended for HPE 3PAR Operating System Software 3.2.2.709 (MU6).

Part Number: QL226-99860
Published: May 2018
Edition: 1

Notices

Acknowledgments

Purpose

The HPE 3PAR OS 3.2.2 MU6 Patch 107 provides security updates to disable older Transport Layer Security (TLS) 1.0 and 1.1 protocols.

IMPORTANT: See the **HPE 3PAR OS and Service Processor Software Update Guide (HPE 3PAR OS 3.2.x HPE 3PAR Service Processor 4.x)** for instructions on updating your specific software.

Guidance

This is an as-needed patch for HPE 3PAR OS 3.2.2 MU6 P107.

Prerequisites

- Minimum SP Version: SP-4.4.0.GA-88
- Base OS: OS-3.2.2.709-MU6. See the Requires field in the Patch details.

  CAUTION: Ensure the customer's host applications that use the affected components are TLS v1.2 compliant (see the Affected components section). Failure to do so may cause the host applications to stop communicating with the array.

  IMPORTANT: If the policy for Common Information Model (CIM) is changed, the cimserver must be restarted for the new policy setting to take effect.

  NOTE: If the customer strictly requires TLS v1.2 only, including client actions, the SP must be using the Remote Device Access (RDA), as the Secure Service Architecture (SSA) is not capable of TLS v1.2 at this time.

Patch details

Patch ID: P107

Synopsis: Changes to support PCI-DSS

Date: May 11, 2018, 15:19:53 PDT

Affected Packages: tpd-api, tpd-cli, tpd-libcli, tpd-libtpdapi, tpd-libtpdtcl, tpd-update, tpd-vasa, tpd-wsapi, tpd-enabletlsstrict, tpd-prerevert

Obsoletes: None

Requires: OS-3.2.2.709-MU6, OS-3.2.2.709-P99

Patches Partially Superseded: OS-3.2.2.709-P99

Patches Included: None

Patches Obsolete by Combination: None

Support Revert: Yes

Build Version: 3.2.2.739

Notes:

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

Modifications

Issue ID	Description
150103 150105 230678 231985	Security improvements to disable older TLS protocols. TLS 1.2 only is supported.

Supported ciphers

In strict TLS1.2 mode CIM and WSAPI support only the following ciphers:

```
DHE-RSA-AES256-GCM-SHA384       DHE-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES256-SHA384         ECDHE-RSA-AES256-SHA384
ECDHE-RSA-AES256-SHA
```

In strict TLSv1.2 mode VASA/VVOL supports the following cipher suites:

```
ECDHE-RSA-AES256-GCM-SHA384      ECDHE-RSA-AES256-SHA384
DH-DSS-AES256-GCM-SHA384         DHE-DSS-AES256-GCM-SHA384
DH-RSA-AES256-GCM-SHA384         DHE-RSA-AES256-SHA384
DHE-RSA-AES256-SHA256            DHE-DSS-AES256-SHA256
DH-RSA-AES256-SHA256             DH-DSS-AES256-SHA256
ECDH-RSA-AES256-GCM-SHA384       ECDH-RSA-AES256-SHA384
AES256-GCM-SHA384                AES256-SHA256
ECDHE-RSA-AES128-GCM-SHA256      ECDHE-RSA-AES128-SHA256
DH-DSS=AES128-GCM-SHA256         DHE-DSS-AES128-GCM-SHA256
DH-RSA-AES128-GCM-SHA256         DHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-SHA256            DHE-DSS-AES128-SHA256
DH-RSA-AES128-SHA256             DH-DSS-AES128-SHA256
ECDH-RSA-AES128-GCM-SHA256       ECDH-RSA-AES128-SHA256
AES128-GCM-SHA256                AES128-SHA256
```

The patches restrict `tpdtcl` to TLSv1.2, and the support of the following ciphers:

```
DHE-RSA-AES256-SHA               DHE-RSA-AES128-SHA
AES256-SHA                       AES128-SHA
```

Affected components

Component	Version
CLI Server	3.2.2.728 (P107)
CIM Server	3.2.2.728 (P107)
WSAPI Server	3.2.2.728 (P107)
Software Updater	3.2.2.728 (P107)
VASA Provider	2.2.11 (P107)

NOTE:

Applying an HPE 3PAR OS patch can cause a restart of the affected OS components. When components are restarted, events and alerts are generated and this is an expected behavior. The system continues to serve data, but existing CLI, SSMC or VASA sessions could be interrupted.

Known issue

Known Issue ID	Description
233007	A message can be seen during the installation of the patch. This message can safely be ignored: Warning Interface definition mismatch for the following interface variables `wsapiInfoInd`.

Verification

The installation of P107 can be verified from an interactive CLI session. Issue the `showversion -a -b` CLI command to verify that P107 is listed:

```
Release version 3.2.2.709 (MU6)
Patches:  P99,P107

Component Name                   Version
CLI Server                       3.2.2.739 (P107)
CLI Client                       3.2.2.739
System Manager                   3.2.2.725 (P99)
Kernel                           3.2.2.709 (MU6)
TPD Kernel Code                  3.2.2.709 (MU6)
TPD Kernel Patch                 3.2.2.725 (P99)
CIM Server                       3.2.2.739 (P107)
WSAPI Server                     3.2.2.739 (P107)
Console Menu                     3.2.2.709 (MU6)
Event Manager                    3.2.2.709 (MU6)
Internal Test Tools              3.2.2.709 (MU6)
LD Check Tools                   3.2.2.709 (MU6)
Network Controller               3.2.2.725 (P99)
Node Disk Scrubber               3.2.2.709 (MU6)
PD Scrubber                      3.2.2.709 (MU6)
Per-Node Server                  3.2.2.725 (P99)
```

```
Persistent Repository            3.2.2.709 (MU6)
Powerfail Tools                  3.2.2.709 (MU6)
Preserved Data Tools             3.2.2.709 (MU6)
Process Monitor                  3.2.2.709 (MU6)
Rolling Upgrade Tools            3.2.2.709 (MU6)
Software Updater                 3.2.2.739 (P107)
TOC Server                       3.2.2.725 (P99)
VV Check Tools                   3.2.2.725 (P99)
File Persona                     1.2.4.3-20170601
SNMP Agent                       1.8.0
SSH                              6.6p1-4~bpo70+1
VASA Provider                    2.2.11 (P107)
Firmware Database                3.2.2.709 (MU6)
Drive Firmware                   3.2.2.709 (MU6)
UEFI BIOS                        04.08.39
MCU Firmware (OKI)               4.8.29
MCU Firmware (STM)               5.2.53
Cage Firmware (DC1)              4.44
Cage Firmware (DC2)              2.64
Cage Firmware (DC3)              08
Cage Firmware (DC4)              2.64
Cage Firmware (DCN1)             4078
Cage Firmware (DCN2)             4078
Cage Firmware (DCS1)             4078
Cage Firmware (DCS2)             4078
Cage Firmware (DCS5)             2.86
Cage Firmware (DCS6)             2.86
Cage Firmware (DCS7)             4078
Cage Firmware (DCS8)             4078
QLogic QLA4052C HBA Firmware     03.00.01.77
QLogic QLE8242 CNA Firmware      04.15.08
QLogic 8300 HBA FC Firmware      08.01.05
QLogic 8300 HBA FCoE Firmware    08.01.05
QLogic 8300 HBA iSCSI Firmware   05.07.07
Emulex LP11002 HBA Firmware      02.82.x10
Emulex LPe12002 HBA Firmware     02.10.x03
Emulex LPe12004 HBA Firmware     02.10.x03
Emulex LPe16002 HBA Firmware     10.6.248.8
Emulex LPe16004 HBA Firmware     10.6.248.8
3PAR FC044X HBA Firmware         200A8
LSI 9201-16e HBA Firmware        17.11.00
LSI 9205-8e HBA Firmware         17.11.00
LSI 9300-8e HBA Firmware         07.10.01
```

NOTE: When displaying the `showversion` command output from the SP, the CLI Client version is fixed 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 for your product or to view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products* reference document, go to the Enterprise Safety and Compliance website:

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

Additional warranty information

HPE ProLiant and x86 Servers and Options

www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise 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.