



Product Support Notice

© 2015 Avaya Inc. All Rights Reserved.

PSN # PSN004481u

Original publication date: 22-Apr-15. This is Issue #01, published date: 22-Apr-15.

Severity/risk level

Medium

Urgency

Optional

Name of problem Session Manager HP DL360P G8 server locks up, fails reboot, or fails during boot and iLO Cipher Suite 0 vulnerability remediation

Products affected

Avaya Aura® Session Manager: Release 6.3.X

Problem description

Some customers have experienced issues related to HP Proliant DL360P G8 servers encounter sudden server lockups requiring cold reboots of the servers to restore service. HP suggests firmware updates to resolve some issues with older versions of firmware and iLO. Due to the sporadic nature of some of these server issues, Session Manager CPE engineers have been unable to reproduce the exact failures experienced by some customers in the field. The firmware that shipped with the G8 servers initially is version 2.2 which includes iLO 1.22. HP recommends going with later versions of their firmware as they have addressed some stability issues since the iLO 1.22 release. The Avaya Common Server Team has provided the HP Proliant DL360P G8 server firmware version 4 DVD to the Session Manager CPE team, and that firmware was load and sanity tested with the latest Session Manager software. No issues with stability were encountered during this testing, and CPE has approved use of the DL360P G8 firmware version 4 with Session Manager 6.3 and later based software loads. If a Session Manager DL360P G8 server experiences a spontaneous shutdown, spontaneous reboots, or kernel panics after a soft reboot, then this firmware upgrade should be applied first to see if it resolves the issue. It should be noted that in some cases this update may not resolve the issue if there is actually a physical hardware problem with the server, which would require a server replacement.

This update to the firmware also addresses the Cipher Suite 0 security issue (CVE-2013-4805 [SSRT1012509]) as well.

Resolution

Download the below referenced DL360P G8 version 4 ISO image, burn it to a DVD and boot the Session Manager G8 server with this DVD to upgrade the firmware/iLO to the latest approved release. This will update the below components to the listed firmware versions:

Device Information		Firmware package release	Firmware Version
iLO 4		CP025108.scexe	V2.03
Power Management Control		CP021615.scexe	V3.3
Power Management Control		CP021012.scexe	V1.6
P71 BIOS (DL360PG8)		CP024481.scexe	2014.08.02
P72 BIOS (DL380PG8)		CP024431.scexe	2014.08.02
P420i SMART ARRAY Cntrl (RAID Controller)		CP023886.scexe	V6.00
HP NC Series Broadcom Firmware (331FLR and 332T)		CP023977.scexe	2.13.5
HP NC Series Broadcom Firmware (331FLR and 332T)		CP0131168.scexe	2.2.7
HDD Firmware Models: EG0146FAWHU, EG0300FAWHV, DG0146FAMWL, DG0300FAMWN		CP020194.scexe	HPDF(C)
HDD Firmware Models: EH0146FCBVB and EH0300FCBVC Drives		CP023185.scexe	HPD4
HDD Firmware Models: EH0146FBQDC and EH0300FBQDD Drives		CP023184.scexe	HPD3
HDD Firmware Models: EH0072FARWC and EH0146FARWD Drives		CP023183.scexe	HPDD
HDD Firmware Models: EH0072FARUA and EH0146FARUB Drives		CP023182.scexe	HPD9

[Type text]

HDD Firmware Models: EG0300FBVFL, EG0450FBVFM, EG0600FBVFP, and EG0900FBVFQ Drives	CP021542.scexe	HPD9
HDD Firmware Models: EG0300FBVFL, EG0450FBVFM, EG0600FBVFP, and EG0900FBVFQ Drives	CP023179.scexe	HPDC
HDD Firmware Models: EG0300FCVBF, EG0450FCVBH, EG0600FCVBK, and EG0900FCVBL Drives	CP023180.scexe	HPD5
HDD Firmware drives Models: EG0300FBDBR, EG0450FBDBT and EG0600FBDBU	CP017743.scexe	HPD7
HDD Firmware drives Models: EG0300FBDBR, EG0450FBDBT and EG0600FBDBU	CP015559.scexe	HPD6
HDD Firmware Models: EG0300FBLSE, EG0450FBLSF, EG0600FBLSH, and EG0900FBLSK Drives	CP023178.scexe	HPD7
HDD Firmware Drives Models: EG0300FBDBR, EG0450FBDBT and EG0600FBDBU	CP023176.scexe	HPDA
HDD Firmware Drives Models: EF0300FARMU, EF0450FARMV, and EF0600FARNA	CP023174.scexe	HPD6
HDD Firmware Models: EF0300FATFD, EF0450FATFE, and EF0600FATFF Drives	CP023175.scexe	HPDB
HDD Firmware Models: DH0072FAQRD, DH0146FAQRE, EH0146FAWJB, and EH0072FAWJA Drives	CP023173.scexe	HPDJ
HDD Firmware Models: DG0146FARVU, DG0300FARVV, DG0146BAMYQ, DG0300BAMYR, EG0146FAWJC, and EG0300FAWJD Drives	CP023172.scexe	HPDG
HDD Firmware Drives Models: EG0300FBDSP, EG0450FBDSQ, and EG0600FBDSR	CP023177.scexe	HPD6

Workaround or alternative remediation

n/a

Remarks

n/a

Patch Notes

The information in this section concerns the patch, if any, recommended in the Resolution above.

Backup before applying the patch

Application of this firmware update requires the Session Manager to be rebooted with the v4 firmware update DVD in the system, thus making this a service affecting update. The Session Manager should be placed in a Deny New Service state before rebooting the server for the firmware update.

Download

The DL360P G8 version 4 update ISO image can be downloaded from PLDS via download ID SM000000079: Session Manager HP DL360P G8 v4 Firmware Update ISO

Patch install instructions

Service-interrupting?

Download the ISO image and burn it to physical media with your favorite burning software. Then follow the below procedures to update all applicable components to their latest firmware versions:

Yes

- 1) A KVM or keyboard/monitor/mouse connected to the G8 server is required to complete this update procedure.
- 2) Insert the DL360PG8 Version 4 firmware update DVD into the DVD drive of the server

- 3) Place the Session Manager server into a Deny New Service state from the System Manager > Elements > Session Manager > Dashboard screen. Wait for the active call count on the server to reach 0 or at least close to zero before proceeding.
- 4) Reboot the Session Manager server from the System Manager > Elements > Session Manager > Dashboard screen.
- 5) Allow the system to boot and load the update utility. After some boot status messages are displayed, a screen will display prompting for the preferred language and a EULA acceptance. Select English and click the “Accept” checkbox and click the Next button on the lower right.
- 6) When the screen showing “Firmware Update”, “HP Smart Storage Administrator”, and “Insight Diagnostics” is displayed, click on the “Firmware Update” icon and the HP System Update Manager will start.
- 7) HP SUM will perform an inventory check of the system which will take a few minutes. When that completes, click on the Next button to continue with the upgrade process.
- 8) The next screen will show a list of components that will be updated. Scroll to the bottom of the list, and click on the “Deploy” button to begin upgrading the components.
- 9) The Step 3 status screen will display the progress of the updates
- 10) Once all updates are applied, a deployment summary screen will be displayed. At the bottom of that list, click on the “Reboot” button to restart the server.
- 11) When possible (after initial FW/Post is done) eject the DVD from the drive via the manual eject button on the front of the drive. The DVD must be removed from the drive before the system attempts to boot, otherwise it will boot the DVD again.
- 12) Once the server reboots, access the System Manager > Elements > Session Manager > System Tools > Maintenance Tests screen, select the Session Manager server that was just updated, and Execute All Tests to ensure that the Session Manager has fully booted and is in a healthy state.
- 13) After maintenance tests have passed, place the Session Manager back into an Accept New Service state from the System Manager > Elements > Session Manager > Dashboard screen.

Verification

Verification that the firmware has been upgraded can be confirmed a couple ways. One is via the console at boot time, the screen will show the ILO FW version which should read 2.3 after the upgrade is applied.

iLO 4 Standard

iLO v**2.03** Nov 07 2014 nnn.nnn.nnn.nnn

Another way if root access to the system is possible, the following command can be run:

```
# dmidecode | grep "Firmware Revision"
```

Firmware Revision: 2.3

And if local access and root access are not available, an sm-report command can be run as craft/cust account. The sm-report output file can then be downloaded to a client machine, and extract the tgz file and view the **dmidecode.out** file within the smreport archive. Search that file for “Firmware Revision:” and the same entry shown above should be in that file.

Failure

n/a

Patch uninstall instructions

n/a

Security Notes

The information in this section concerns the security risk, if any, represented by the topic of this PSN.

Security risks

Cipher Suite 0 vulnerability is resolved by this firmware update as well. Details of this vulnerability can be found at http://h20564.www2.hp.com/hpsc/doc/public/display?docId=emr_na-c03844348

Avaya Security Vulnerability Classification

Low

Mitigation

Upgrade to the HP DL360P G8 Firmware version 4 referenced in this PSN.

If you require further information or assistance please contact your Authorized Service Provider, or visit support.avaya.com. There you can access more product information, chat with an Agent, or open an online Service Request. Support is provided per your warranty or service contract terms unless otherwise specified in the Avaya support [Terms of Use](#).

Disclaimer: ALL INFORMATION IS BELIEVED TO BE CORRECT AT THE TIME OF PUBLICATION AND IS PROVIDED “AS IS”. AVAYA INC., ON BEHALF OF ITSELF AND ITS SUBSIDIARIES AND AFFILIATES (HEREINAFTER COLLECTIVELY REFERRED TO AS “AVAYA”), DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND FURTHERMORE, AVAYA MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE STEPS RECOMMENDED WILL ELIMINATE SECURITY OR VIRUS THREATS TO CUSTOMERS’ SYSTEMS. IN NO EVENT SHALL AVAYA BE LIABLE FOR ANY DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THE INFORMATION OR RECOMMENDED ACTIONS PROVIDED HEREIN, INCLUDING DIRECT, INDIRECT, CONSEQUENTIAL DAMAGES, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF AVAYA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE INFORMATION PROVIDED HERE DOES NOT AFFECT THE SUPPORT AGREEMENTS IN PLACE FOR AVAYA PRODUCTS. SUPPORT FOR AVAYA PRODUCTS CONTINUES TO BE EXECUTED AS PER EXISTING AGREEMENTS WITH AVAYA.

All trademarks identified by ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc.
All other trademarks are the property of their respective owners.