Product Support Notice

© 2018 Avaya Inc. All Rights Reserved.

PSN #	PSN027066u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.

Original publication date: 07-May-18. This is Issue #1, published date: 07-May-18.		Severity/risk level	Medium	Urgency	When convenient
Name of problem	PSN027066u – Avaya Common Server R3 (HPE DL20/DL360/380 G9) and R2 (DL360p/380p G8) Meltdown and Spectre Vulnerabilities				

Products affected

Common Server R3 (HPE DL20/DL360/380 G9)
Common Server R2 (DL360p/380p G8)
Avaya Aura® Appliance Virtualization Platform 7.x
Avaya Call Management System (CMS) Releases 17-18

Problem description

An industry-wide issue was found in the way many modern microprocessor designs have implemented speculative execution of instructions (a commonly used performance optimization). There are three primary variants of the issue which differ in the way the speculative execution can be exploited. These exploitations/vulnerabilities are commonly referred to as Meltdown and Spectre. Please reference **PSN020346u** for information about mitigation of Spectre and Meltdown vulnerabilities for Avaya Aura® application software.

Resolution

Avaya is providing an Avaya certified update that addresses the Spectre and Meltdown vulnerabilities with the necessary Intel Microcode BIOS updates. Please be aware that the Avaya Aura® Appliance Virtualization Platform hypervisor also provides the Intel Microcode updates. These have the same effect as the BIOS updates included in this package. However, the BIOS version on the server (eg, via smbiosDump) may not reflect the update if installed only from the hypervisor.
It is recommended that this BIOS/Firmware update be applied in addition to the hypervisor update.

NOTE:

- In order to mitigate the Meltdown and Spectre vulnerabilities, the processor manufacturers and operating system developers will need to provide software patches to their products. These are patches to the processors and operating systems, not to Avaya products.
- Once these patches are received by Avaya, Avaya will test these patches with the applicable Avaya products to determine what, if any, impact these patches will have on the performance of the Avaya product.
- Avaya is reliant on our Suppliers to validate the effectiveness of their respective Meltdown and Spectre vulnerability patches.
- Avaya's test effort is targeted towards reaffirming product/solution functionality and performance associated with the deployment of these patches.
- The customer is responsible for implementing, and the results obtained from, such patches.
- The customer should be aware that implementing these patches may result in performance degradation.

In addition to the Intel Microcode BIOS updates, this package also includes updates to iLO, RAID Controller, Power Management Controller, Ethernet NIC and HDD Firmware.

This firmware is customer installable.

NOTE:

- **Avaya OEM servers used in turnkey application offers must <u>NOT</u> be updated with BIOS or firmware updates from the vendor's web site.** Only Avaya-provided updates should be used.
- **You should always utilize the Avaya certified, bundled release**. Do NOT upgrade individual components. HP releases bundles called SPPs (Service Pack for ProLiant). This ensures that the components have been tested together for dependencies. Avaya then creates a tailored HP SPP firmware update tool for our Common Server Configurations that goes through additional testing.

The following procedure describes how to obtain and run the Avaya approved BIOS/firmware update tool on any of the following servers: HPE DL20/DL360/380 G9 and DL360p/380p G8. This firmware update is provided as a bootable, off-line tool that will install new firmware onto the server. When the update tool is run it will indicate firmware versions currently installed on the server.

The user can select to run or not to run the updates at that time. Other methods to check firmware versions on the server are shown at the end of this document.

Acquiring Update Tool

Download the file, ***bp-Avaya-DL360G9-G8-SPP-2017101-6-3.iso*** via PLDS download ID **CMCS0000014** and burn a **bootable** DVD from it.

The example installation screen shots in this document are for an HPE DL360 G9. Other servers will be similar. When the update tool is run it will indicate firmware versions currently installed on the server. After executing the procedures, the following components will be updated to the listed firmware versions.

The DL20/DL360/380 G9 and DL360p/380p G8 Server Firmware update (v6.3) disc contains:

Device Information	Firmware package release	Firmware Version
iLO 4	hp-firmware-ilo4-2.55-1.1.i386.rpm	v2.55
Power Management Controller	hp-firmware-powerpic-gen9-1.0.9-3.i386.rpm	v3.3
P89 BIOS (DL380/360G9)	hp-firmware-system-p89-2.22_2016_07_18-1.1.i386.rpm	v2.56 01/22/2018
P71 BIOS (DL360pG8)	firmware-system-p71-2018.01.22-1.1.i386.rpm	01/22/2018
P70 BIOS (DL380pG8)	firmware-system-p70-2018.01.22-1.1.i386.rpm	01/22/2018
P89 BIOS (DL380/360G9)	firmware-system-p89-2.52_2017_10_25-1.1.i386.rpm	v2.52 10/25/2017
P70 BIOS (DL380pG8)	hp-firmware-system-p70-2015.07.01-1.1.i386.rpm	07/01/2015
P71 BIOS (DL360pG8)	hp-firmware-system-p71-2015.07.01-1.1.i386.rpm	07/01/2015
HPE ProLiant DL20 Gen9 (U22) Servers	u22-2.56_2018_01_22-1.1.i386.rpm	v2.56 01/22/2018
P440ar SMART ARRAY Cntrl (RAID Controller)	firmware-smartarray-ea3138d8e8-6.06-1.1.x86_64.rpm	v6.06
HP NC Series Broadcom Firmware (331i, 331FLR and 332T)	firmware-nic-broadcom-2.20.7-1.1.x86_64.rpm	v20.8.41
HP FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter HP StoreFabric CN1100R Dual Port Converged Network Adapter HP FlexFabric 10Gb 2-port 534FLB Adapter HP FlexFabric 10Gb 2-port 534M Adapter	firmware-nic-qlogic-nx2-2.21.15-1.1.x86_64.rpm	v7.10.72
P420i SMART ARRAY Cntrl (RAID Controller)	hp-firmware-smartarray-46a4d957a7-8.32-1.1.x86_64.rpm	v8.32

© 2018 Avaya Inc. All Rights Reserved.

EG001800JWFVC Drives	firmware-hdd-693b9a2853-HPD2-1.1.x86_64.rpm	HPD2
MB8000GFECR Drives	firmware-hdd-6d922fc9a8-HPG4-2.1.x86_64.rpm	HPG4
MB2000JFDSL and MB4000JFDSN Drives	firmware-hdd-46fc43ab26-HPD3-1.1.x86_64.rpm	HPD3
EG0300JEHLV, EG0600JEHMA, EG0900JEHMB, and EG1200JEHMC Drives	firmware-hdd-31f91b8622-HPD3-3.1.x86_64.rpm	HPD3
VK000240GWEZB, VK000480GWEZC, VK000960GWEZD, VK001920GWEZE, MK000240GWEZF, MK000480GWEZH, MK000960GWEZK, and MK001920GWHRU Drives	firmware-hdd-3db7640485-HPG4-1.1.x86_64.rpm	HPG4
MB006000GWBXQ and MB008000GWBYL Drives	firmware-hdd-a1fd19f9ca-HPG5-1.1.x86_64.rpm	HPG5
EG0300JFCKA, EG0600JEMCV, EG0900JFCKB, and EG1200JEMDA Drives	firmware-hdd-ac3fda26eb-HPD6-2.1.x86_64.rpm	HPD6
MB6000GVYYU Drives	firmware-hdd-bdc37cb37f-HPG2-1.1.x86_64.rpm	HPG2
MB2000GCVBR, MB3000GCVBT, and MB4000GCVBU Drives	firmware-hdd-e4f5b5c9a7-HPG5-3.1.x86_64.rpm	HPG5
MB1000JVYZL, MB2000JVYZN, MB3000JVYZP, and MB4000JVYZQ Drives	firmware-hdd-b85516c7d2-HPD2-1.1.x86_64.rpm	HPD2
MB2000JFEPA and MB4000JFEPB Drives	firmware-hdd-326de7c0f2-HPD5-1.1.x86_64.rpm	HPD5
MB2000GCWLT, MB3000GCWLU, and MB4000GCWLV Drives	firmware-hdd-2e70ce7412-HPG4-2.1.x86_64.rpm	HPG4
MB001000GWFWK and MB002000GWFWL Drives	firmware-hdd-bfc4af697b-HPG4-2.1.x86_64.rpm	HPG4
EH000600JWCPF and EH000900JWCPH Drives	firmware-hdd-a05f29cef3-HPD3-1.1.x86_64.rpm	HPD3
MB4000GEQNH and MB6000GEQNK Drives	firmware-hdd-bfc95f0628-HPG7-3.1.x86_64.rpm	HPG7
MB6000JVYYV Drives	firmware-hdd-0595c2a887-HPD2-1.1.x86_64.rpm	HPD2
MO0200JEFNV, MO0400JEFPA, MO0800JEFPB, MO1600JEFPC, EO0200JEFPD, EO0400JEFPE, and EO0800JEFPF Drives	firmware-hdd-71af849f3b-HPD3-1.1.x86_64.rpm	HPD3
MB6000GEXXV Drives	firmware-hdd-a629fcea59-HPG2-2.1.x86_64.rpm	HPG2
EG0600JETKA, EG0900JETKB, and EG1200JETKC Drives	firmware-hdd-7505dfb5ae-HPD6-1.1.x86_64.rpm	HPD6
EH0300JEDHC, EH0450JEDHD, and EH0600JEDHE	firmware-hdd-8c4a212ff9-HPD4-	HPD4

© 2018 Avaya Inc. All Rights Reserved.

Drives	2.1.x86_64.rpm	
MR000240GWFLU, MR000480GWFLV, VR000480GWFMD, MR000960GWFMA, VR000960GWFME, MR001920GWFMB, and VR001920GWFMC Drives	firmware-hdd-9196d4f720-HPG4-1.1.x86_64.rpm	HPG4
MM1000JEFRB and MM2000JEFRC Drives	firmware-hdd-b04257b77b-HPD7-1.1.x86_64.rpm	HPD7
MB6000GEBTP Drives	firmware-hdd-3243fce9a0-HPG3-1.1.x86_64.rpm	HPG3
XP0032GEFEN, XP0032GDZME, XP0064GEFEP, and XP0064GDZMF Drives	firmware-hdd-f286f98973-HPS8-2.1.x86_64.rpm	HPS8
EH0300JDXBA, EH0450JDXBB, and EH0600JDXBC Drives	firmware-hdd-1cbab97ff0-HPD5-1.1.x86_64.rpm	HPD5
EG1800JEHMD Drive	firmware-hdd-8a2c06af48-HPD4-4.1.x86_64.rpm	HPD4
MB1000GDUNU, MB2000GDUNV, MB3000GDUPA, and MB4000GDUPB Drives	firmware-hdd-3ab4c70e64-HPG4-2.1.x86_64.rpm	HPG4
EG1800JEMDB Drives	firmware-hdd-0a38b25661-HPD3-1.1.x86_64.rpm	HPD3
MK0960GECQK Drives	firmware-hdd-3e34285be7-HPG3-3.1.x86_64.rpm	HPG3
MM1000GEFQV and MM2000GEFRA Drives	firmware-hdd-ec908c3650-HPG5-1.1.x86_64.rpm	HPG5
VO1920JEUQQ Drives	firmware-hdd-5d9e841607-HPD3-1.1.x86_64.rpm	HPD3
MB001000GWCBC and MB002000GWCBD Drives	firmware-hdd-68b12e54d2-HPG4-2.1.x86_64.rpm	HPG4
EG000300JWBHR Drives	firmware-hdd-2e4c61fc63-HPD3-2.1.x86_64.rpm	HPD3
MM1000GFJTE Drives	firmware-hdd-95af9a555e-HPG1-2.1.x86_64.rpm	HPG1
EG000600JWEBH and EG000300JWEBF Drives	firmware-hdd-aa9e289524-HPD3-1.1.x86_64.rpm	HPD3
EH000300JWCPK, EH000600JWCPL, and EH000900JWCPN Drives	firmware-hdd-3d97759111-HPD3-1.1.x86_64.rpm	HPD3
MB1000GCWCV, MB2000GCWDA, MB3000GCWDB, and MB4000GCWDC Drives	firmware-hdd-a1b08f8a6b-HPGI-2.1.x86_64.rpm	HPGI
XP0120GFJSL and XP0240GFJSN Drives	firmware-hdd-d355375539-HPS4-2.1.x86_64.rpm	HPS4
MM1000JFJTH Drives	firmware-hdd-fa46c607d6-HPD2-1.1.x86_64.rpm	HPD2

© 2018 Avaya Inc. All Rights Reserved.

MB4000JEXYA and MB6000JEXYB Drives	firmware-hdd-0f923833e9-HPD8-1.1.x86_64.rpm	HPD8
MB4000JEFNC and MB6000JEFND Drives	firmware-hdd-af802bb412-HPD9-1.1.x86_64.rpm	HPD9
MB1000GVYZE, MB2000GVYZF, MB3000GVYZH, and MB4000GVYZK Drives	firmware-hdd-0a7010918e-HPG4-2.1.x86_64.rpm	HPG4
MB6000JEQUV and MB8000JEQVA Drives	firmware-hdd-df22f7effd-HPDB-1.1.x86_64.rpm	HPDB
VK0120GFDKE, VK0240GFDKF, VK0480GFDKH, VK0960GFDKK, VK1920GFDKL, and VK3840GFDKN Drives	firmware-hdd-a2d4b5c742-HPG1-2.1.x86_64.rpm	HPG1
EG1800JFHMH Drives	firmware-hdd-7fc5497116-HPD5-2.1.x86_64.rpm	HPD5
MB4000GEFNA and MB6000GEFNB Drives	firmware-hdd-40277d55d3-HPG6-1.1.x86_64.rpm	HPG6
MB8000JFECQ Drives	firmware-hdd-252770cdda-HPD4-2.1.x86_64.rpm	HPD4
MB0500GCEHF, MB1000GCEHH, and MB2000GCEHK Drives	firmware-hdd-b583d96f94-HPGD-5.1.x86_64.rpm	HPGD
MB4000JEQNL and MB6000JEQNN Drives	firmware-hdd-2cfaac41db-HPD7-3.1.x86_64.rpm	HPD7
EG0300FCSPH, EG0450FCSPK, EG0600FCSPL, and EG0900FCSPN Drives	firmware-hdd-7c1a1734f9-HPD2-1.1.x86_64.rpm	HPD2
EH0300JDYTH, EH0450JDYTK, and EH0600JDYTL Drives	firmware-hdd-b9340d29be-HPD4-3.1.x86_64.rpm	HPD4
MR000240GWFLU, MR000480GWFLV, VR000480GWFMD, MR000960GWFMA, VR000960GWFME, MR001920GWFMB, and VR001920GWFMC Drives	firmware-hdd-9196d4f720-HPG6-1.1.x86_64.rpm	HPG6
EG1800JFHMH Drives	firmware-hdd-7fc5497116-HPD6-1.1.x86_64.rpm	HPD6
EH0300JDYTH, EH0450JDYTK, and EH0600JDYTL Drives	firmware-hdd-b9340d29be-HPD6-1.1.x86_64.rpm	HPD6
EH0600JDYTN Drive	firmware-hdd-f3faa195ff-HPD7-1.1.x86_64.rpm	HPD7
EG1800JEHMD Drive	firmware-hdd-8a2c06af48-HPD6-1.1.x86_64.rpm	HPD6
EG0300JEHLV, EG0600JEHMA, EG0900JEHMB, and EG1200JEHMC Drives	firmware-hdd-31f91b8622-HPD5-1.1.x86_64.rpm	HPD5

Note: HDD firmware is included in the update disc to cover all possible HDD models that may have shipped in a DL360G9 server. A server may not require any, and will not require all HDD firmware packages on this disc. If that is the case, it will skip that update process.

© 2018 Avaya Inc. All Rights Reserved.

Acquiring Update Tool

Download the file, ***bp-Avaya-DL360G9-G8-SPP-2017101-6-3.iso*** via PLDS download ID **CMCS0000014** and burn a **bootable** DVD from it.

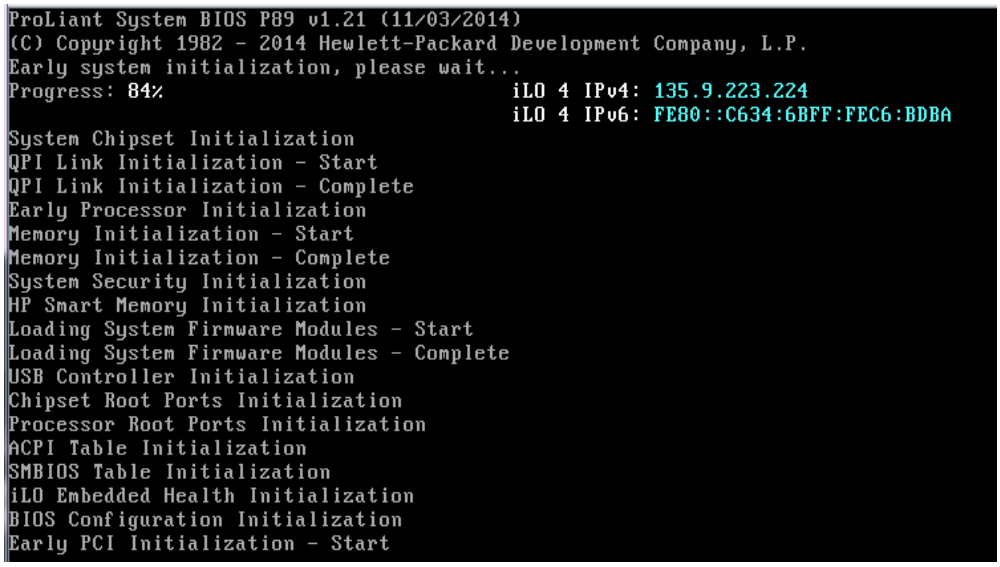
BIOS/Firmware Update Procedures

The example screen shots below are for an HPE DL360 G9. Other server models will be similar.

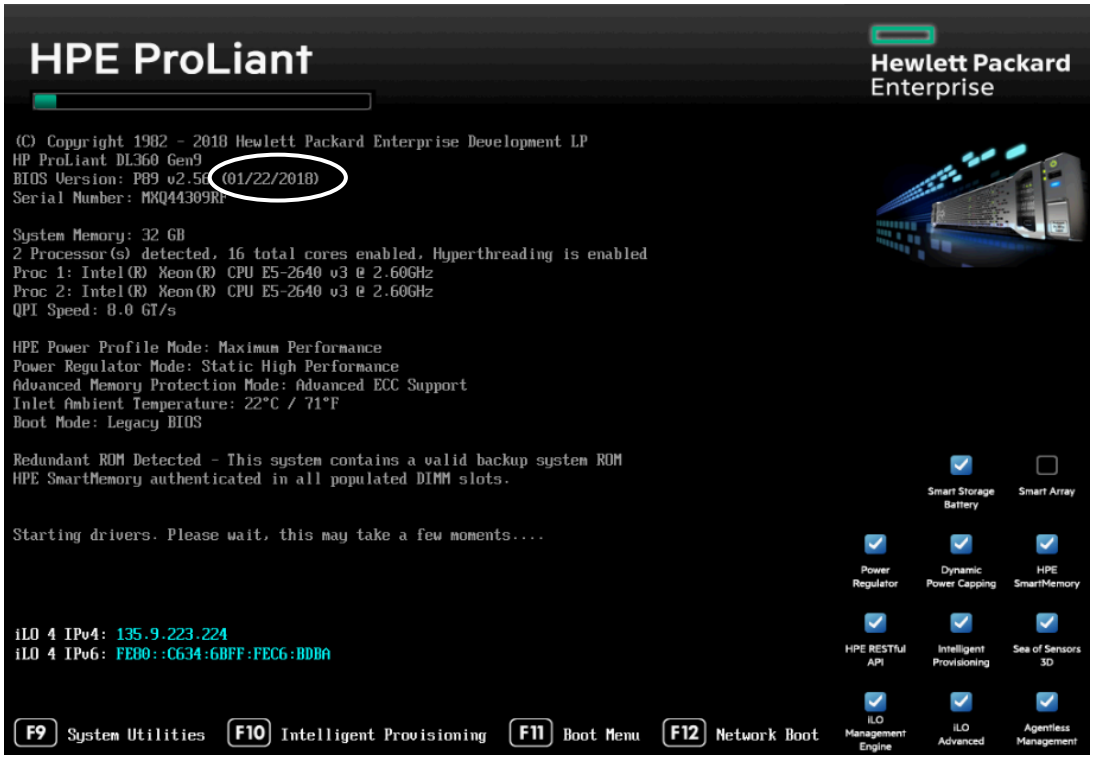
It is always best practice to perform a complete backup of the system before any firmware or hardware maintenance. It is recommended to do a system reboot prior to initiating the BIOS/Firmware update procedure. This will decrease the update execution time.

Gracefully shut down the server according to Application Procedures

1. A monitor, USB keyboard and mouse will be required to run the update tool.
2. Insert the firmware update disc at server power up.

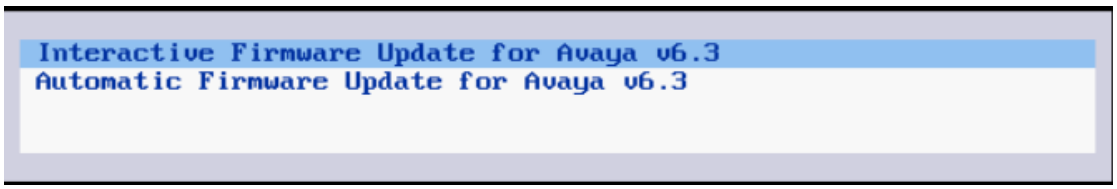


3. Hardware boot screens will appear.



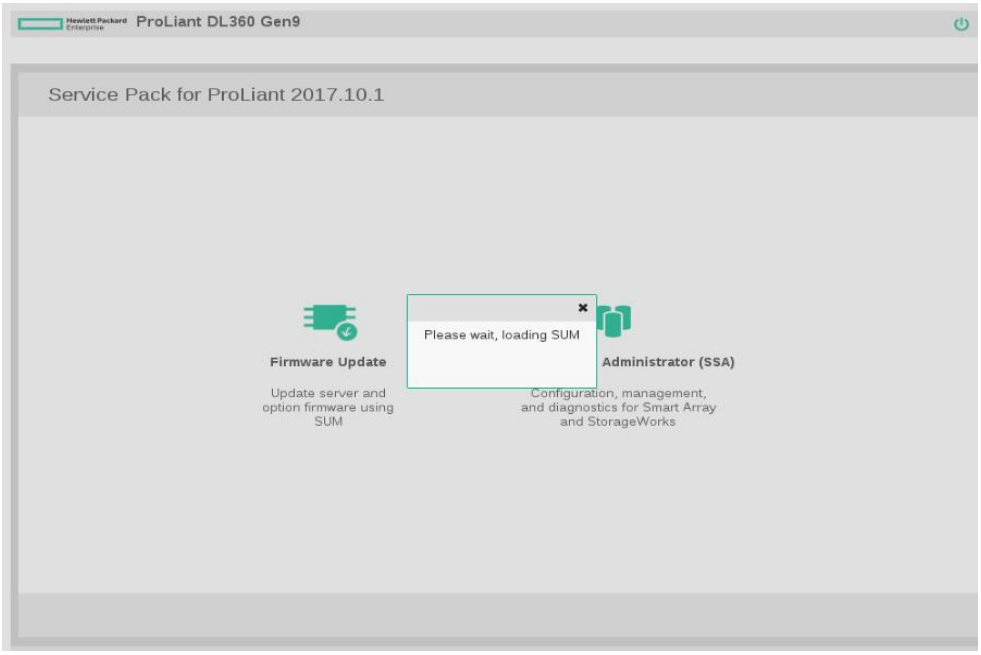
© 2018 Avaya Inc. All Rights Reserved.

4. The system will boot from the DVD and load the update utility from the disc. HPE CSR3/CSR2 servers boot in Legacy BIOS mode so the the tool will default to Interactive mode.



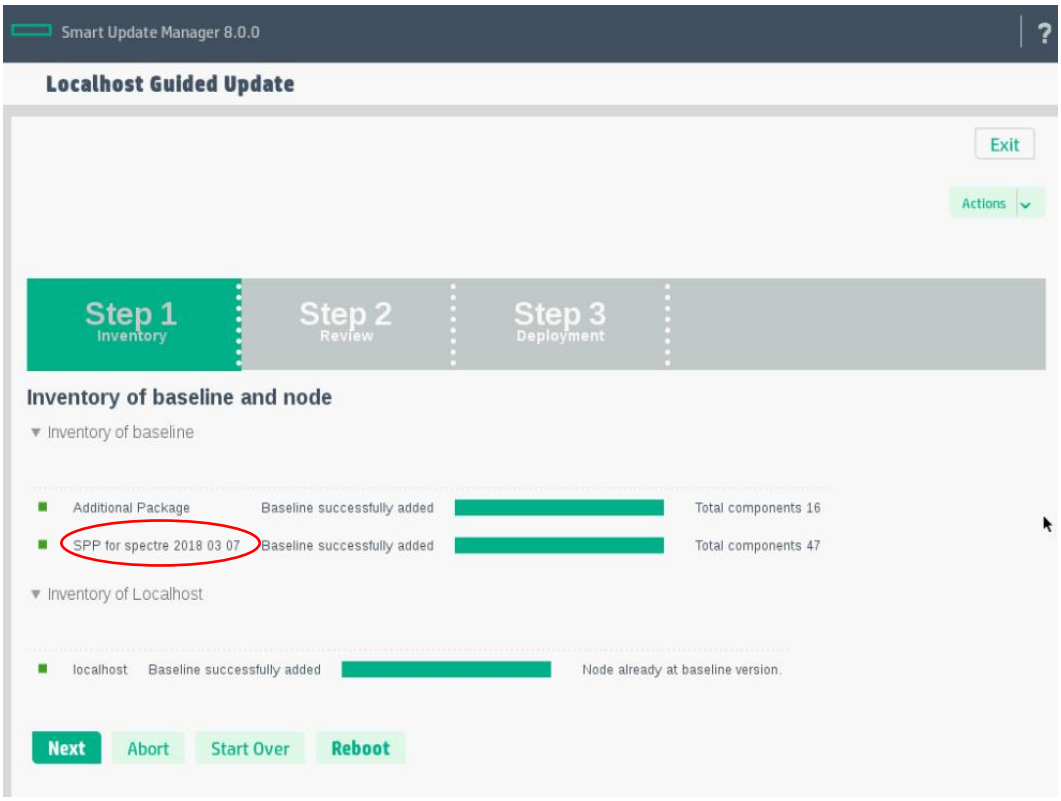
5. Interactive Firmware Update will be selected by default unless interrupted from the keyboard. To change the update mode press space bar to interrupt and use arrow key to select/highlight update mode and then press <ENTER>. Interactive is prefered for updating CSR2 and CSR3 HPE servers.

6. Select language, accept EULA and select <Next>.



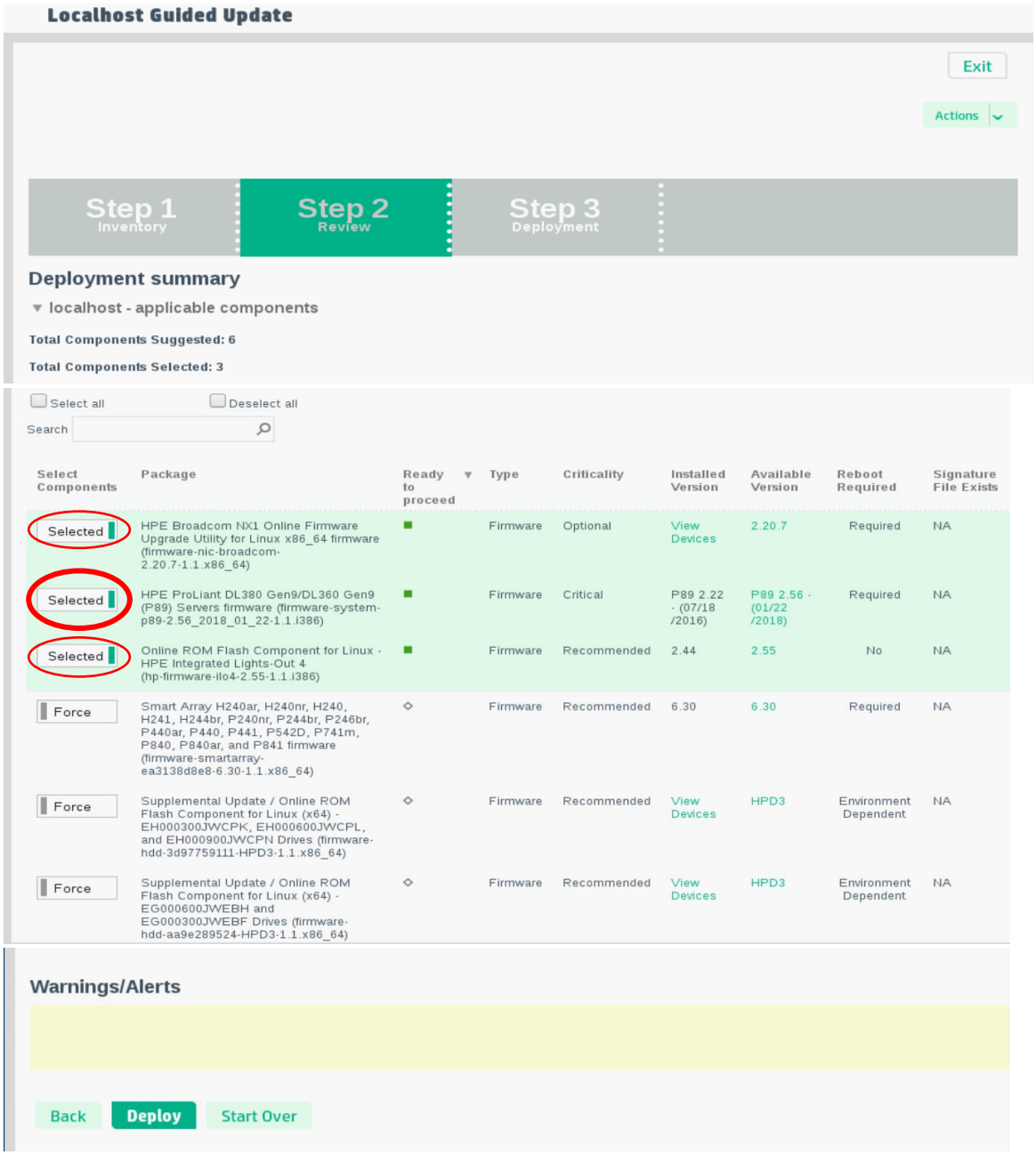
© 2018 Avaya Inc. All Rights Reserved.

7. Select the **Firmware Update** icon. HP SUM will load. This process will take approximately 4 minutes.



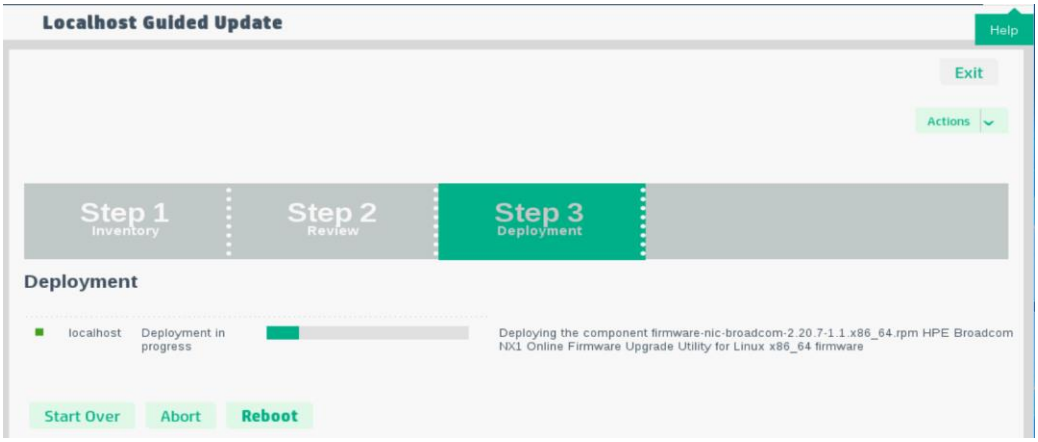
8. A ***No items found!*** message may be momentarily displayed, but will be replaced by an additional package inventory of approximately 47 firmware components suitable for the server available for install. Many updates are for HP HDDs that may not be installed in the server and therefore will not be applicable for update.
9. Select **<Next>** when button becomes highlighted.

© 2018 Avaya Inc. All Rights Reserved.

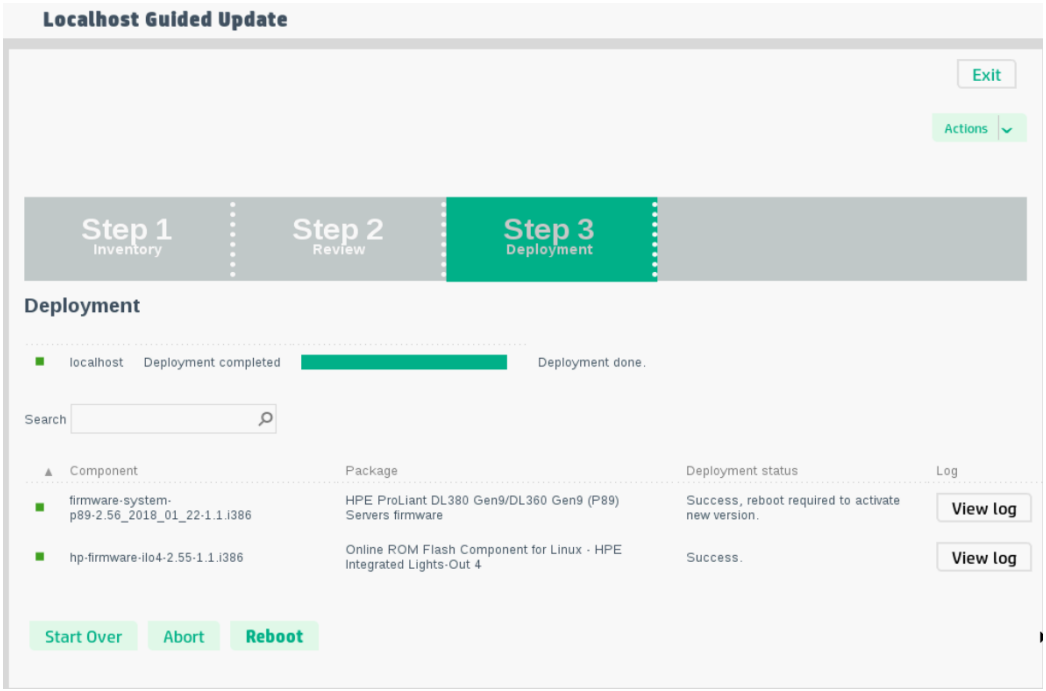


10. Firmware packages similar to what is shown on the above screen will display. The tool will auto select (<**Selected**> buttons circled in **red**) what packages it determines are necessary for upgrade based on version or date. Firmware components on the server that are equivalent to or newer than what is on the update disc should not be selected. In this example HPE Broadcom NX1 NIC device, System ROM(BIOS) and iLO components are selected for update. The Smart Array and two HDD components are not selected for update because they are determined to not require updating. Select <**Deploy**> when ready to upgrade selected firmware components.

© 2018 Avaya Inc. All Rights Reserved.



11. Required updates are being installed



When complete, a page will display showing package deployment status. If one or more packages did not load successfully see next section: ***If a package did not install.*** If all packages successfully installed select the **<Reboot>** button. When server starts to boot up (POST) press the DVD drive eject button to remove the update disc. Select <F9> on HP splash screen to check for firmware versions if desired. See section ***How to Check Firmware Versions on an HP DL360G9*** *or* ***How to Check Firmware Versions on an HP DL360pG8*** below.

<u>If a package did not install:</u>

Select the **<View log>** button to see if prerequisites may not have been met. If a prerequisite is required, please note the information, contact Avaya Services and reference this PSN.

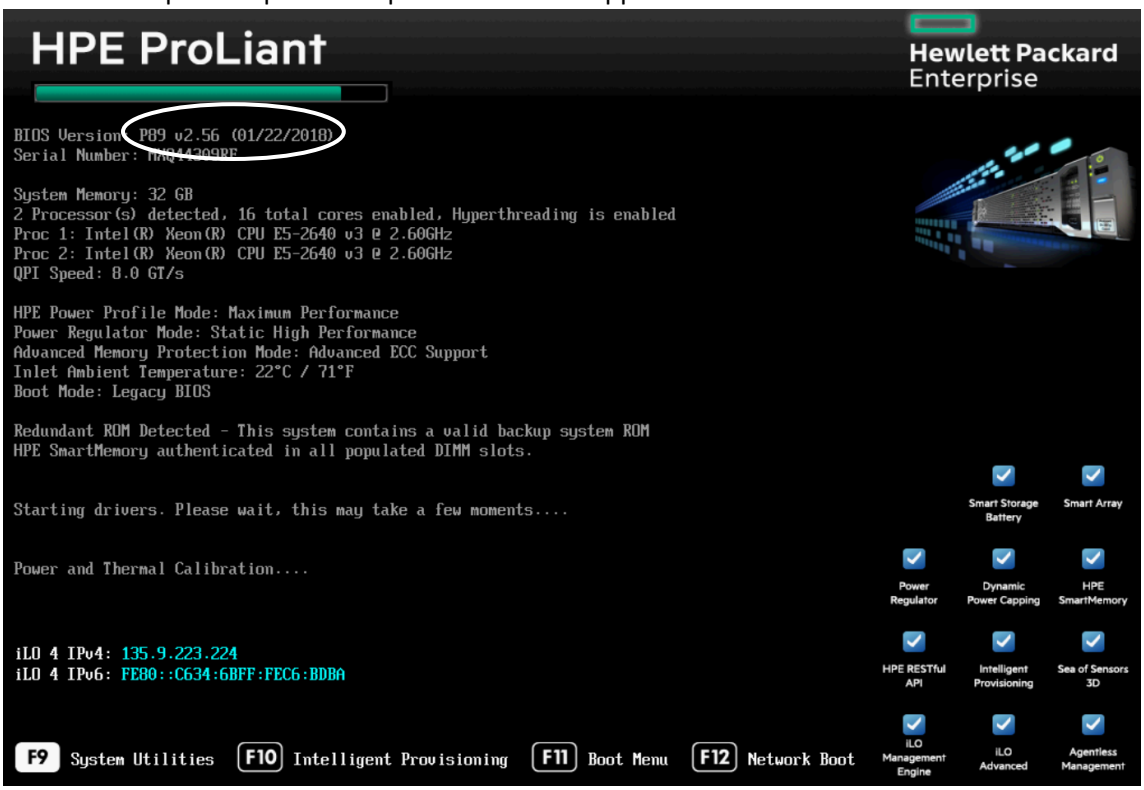
If no prerequisite is mentioned in the log, reboot the server and try to reinstall package(s). If package fails to install a second time, power off server and remove power cord(s). Wait 3 minutes, insert power cords, power up server and re-install packages.

© 2018 Avaya Inc. All Rights Reserved.

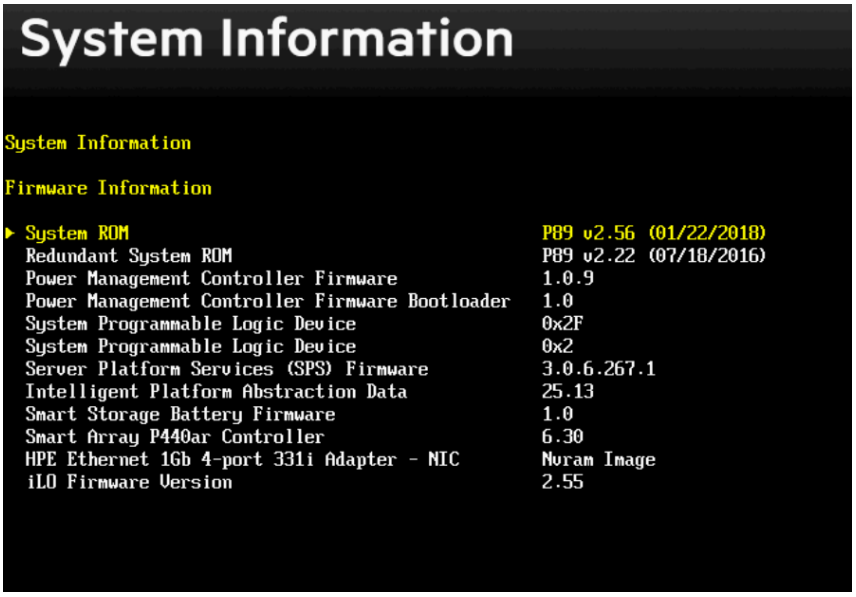
Examples for how to check the firmware version. These are similar, regardless of the server model. Please refer to the table on Page 2 that lists the updates for specific server types to determine what the BIOS version should be.

How to Check Firmware Versions on an HPE DL360G9

1. A Monitor and USB keyboard will be required to check firmware versions.
2. Reboot or power up server. Splash screen will appear as shown below.

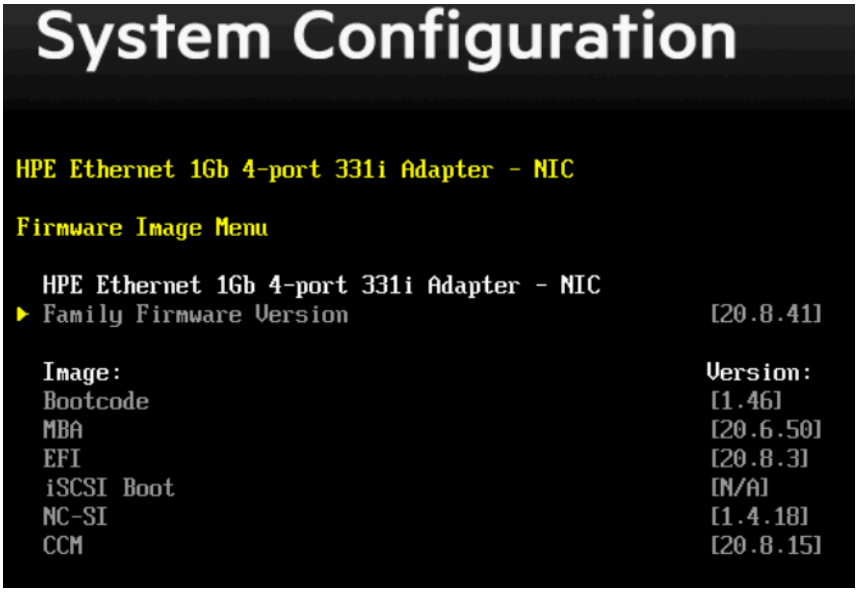


3. Select **<F9>** when available on the HP Splash screen to select **System Utilities**



4. Select **System Information/Firmware Information.** Check System ROM is v2.56, Smart Array P440ar (or P440) Controller is v6.30, iLO is 2.55 and HP Ethernet 1Gb 2-port/4-port 331T/331i Adapter Nvram Image.Report NvRam(translates to v2.8.41 - See Appendix section for more information). Press **<ESC>** to return to top menu.

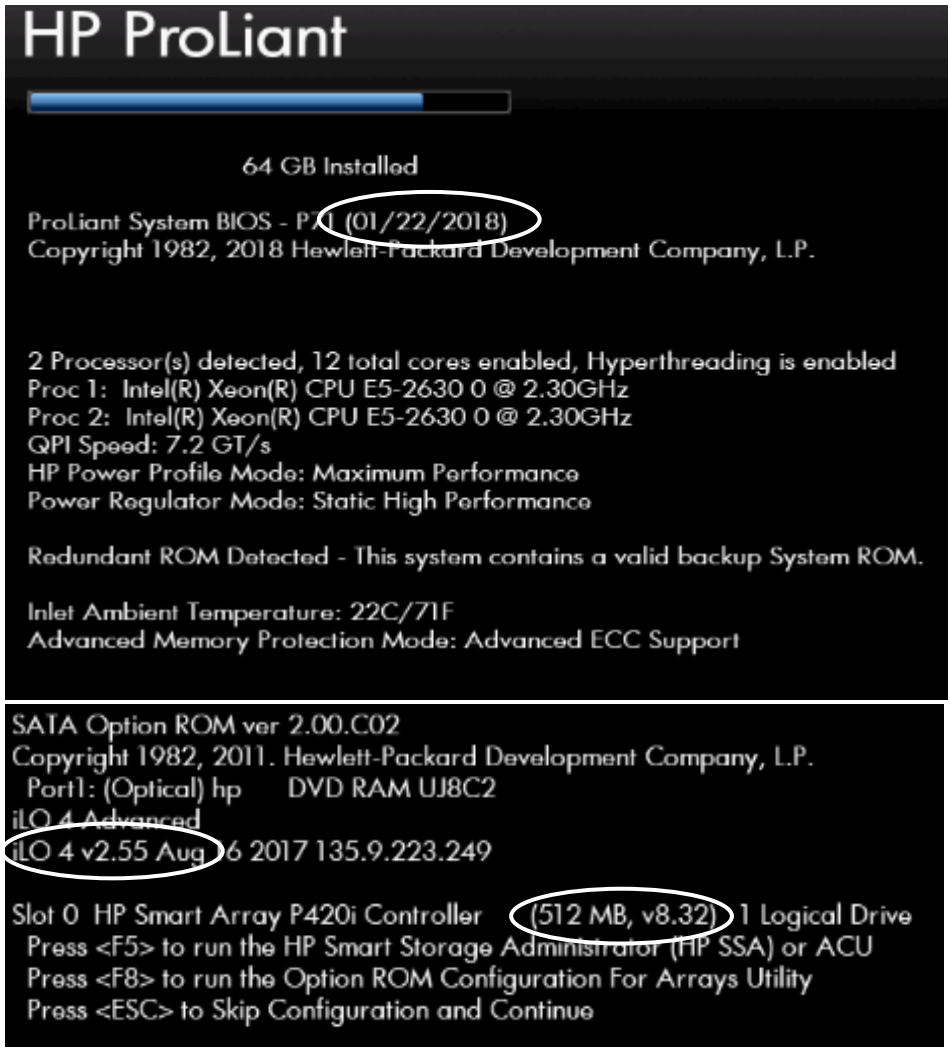
© 2018 Avaya Inc. All Rights Reserved.



5. To check Ethernet 1Gb 4-port 331i Adaptor firmware version select **System Utilities/System Configuration/Embedded LOM 1 Port 1 : HPE Ethernet 1Gb 4-port 331i Adaptor – NIC/Firmware Image Menu.** Additional information can be found in the Appendix section. If 1Gb 2-port 332T Adapter is installed the same sequence by be used to check firmware versions.
6. Press <ENTER> to exit and resume normal boot.

© 2018 Avaya Inc. All Rights Reserved.

Example: How to Check Firmware Versions on an HPE DL360pG8



1. BIOS version 01/22/2018 should be displayed on hardware boot screen
2. iLO 4 v2.55 and P420i Controller v8.32 should be displayed.
3. If NIC card and other packages require confirmation re-run tool in interactive mode and validate with tool's report. Exit tool without running.

For all servers running AVP:

The smbiosDump command can be used from the AVP shell to confirm the BIOS version if it was updated via this procedure. This example is for an HPE DL360 G8 and the updated BIOS is reflected as 01/22/2018.

EG:

```
~admin#smbiosDump | more
Dumping live SMBIOS data!
  BIOS Info: #0
    Size: 0x00018
    Vendor: "HP"
    Version: "P71"
    Date: "01/22/2018"
```

© 2018 Avaya Inc. All Rights Reserved.

Workaround or alternative remediation

N/A.

Remarks

N/A.

Patch Notes

Backup before applying the patch

N/A.

Download

N/A.

Patch install instructions | Service-interrupting?

N/A. | Yes

Verification

N/A.

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

Avaya uses the Common Vulnerability Scoring System version 3 (CVSSv3) base score and metrics as reported by the vendor for the affected component(s) or by the National Institute of Standards and Technology in the National Vulnerability Database. In some cases, such as where CVSS information is not available from the vendor or NIST, Avaya will calculate the CVSSv3 base score and metrics. Customers are encouraged to calculate the Temporal and Environmental CVSSv3 scores to determine how the vulnerability could affect their specific implementation or environment. For more information on CVSS and how the score is calculated, see Common Vulnerability Scoring System v3.0: Specification Document

Vulnerability	CVSSv3 Base Score	CVSSv3 Metrics
CVE-2017-5753	5.6 (Medium)	CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N
CVE-2017-5715	5.6 (Medium)	CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N
CVE-2017-5754	5.6 (Medium)	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N

Avaya Security Vulnerability Classification

Medium.

Mitigation

N/A.

© 2018 Avaya Inc. All Rights Reserved.

For additional support, contact your Authorized Service Provider. Depending on your coverage entitlements, additional support may incur charges. Support is provided per your warranty or service contract terms unless otherwise specified.

Avaya Support Contact	Telephone
U.S. Remote Technical Services – Enterprise	800-242-2121
U.S. Remote Technical Services – Small Medium Enterprise	800-628-2888
U.S. Remote Technical Services – BusinessPartners for Enterprise Product	877-295-0099
BusinessPartners for Small Medium Product	Please contact your distributor.
Canada	800-387-4268
Caribbean and Latin America	786-331-0860
Europe, Middle East, and Africa	36-1238-8334
Asia Pacific	65-6872-8686

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.