Product Support Notice

PSN #	PSN027107u	

Original publication date: 29-Apr-24. This is Issue #1, published date: 29-Apr-24.	**Severity/risk level**	High	**Urgency**	Immediately

Name of problem	PSN027107u - Avaya Solutions Platform 100 Series Dell® R640 Avaya Certified BIOS/Firmware Update, Version 13.0

Products affected

Avaya Solutions Platform 100 Series Dell® R640

NOTE: Avaya Converged Platform (ACP) was rebranded to Avaya Solutions Platform(ASP) in December of 2019

Problem description

Notes:

- Avaya Solutions Platform 100 Series Dell® R640 Avaya Certified BIOS/Firmware Update Version 13.0 BIOS update addresses the following important issues.
  - ➤ CVEs for the iDRAC. Reference [iDRAC9 Version 7.00.00.171 Release Notes (dell.com)](#) for full details of what has changed.
    - ▪ [CVE - CVE-2023-51767 (mitre.org)](#)
    - ▪ [CVE - CVE-2023-51385 (mitre.org)](#)
    - ▪ [CVE - CVE-2023-28531 (mitre.org)](#)
    - ▪ [CVE - CVE-2023-38408 (mitre.org)](#)
    - ▪ [CVE - CVE-2023-48795 (mitre.org)](#)

  - ➤ PERC H750 single or multibit ECC messages per [PERC11: PERC H750, H755, H755N controllers may experience single or multi-bit ECC messages. | Dell Hong Kong](#)

- Avaya certified BIOS/FW updates should be applied as soon as possible to ensure robust security protection, performance, and defense against known issues. BIOS/FW versions should always be checked whenever any maintenance activity is being performed on the server. This would include but is not limited to application updates/upgrades, server swaps, server remastering, new installations. It is recommended that the BIOS/FW update be performed prior to any other activity.

Avaya is providing an approved/certified update bundle for BIOS and Firmware on the ASP 100 Series Dell® R640 servers. This is inclusive of ASP 110, ASP 120, ASP 130 with the *following exceptions* for ASP 110.

Code	Description
700514273	ASP 110 DELL R640 SRVR P5 EQX SNR
700514861	ASP 110 DELL R640 SRVR P5 ACCS

This bundle is designated **Version 13.0** and is customer installable.

Avaya Solutions Platform 100 Series Dell® R640 servers are supplied under OEM relationship and managed differently than commercially available servers from the vendor.

Support, warranty and repair are through Avaya's processes, not through the OEM vendor's support process.

ASP 100 Series Server configurations are engineered for specific application needs. No hardware substitutions or additions are allowed. **Servers cannot be repurposed.**

Lifecycle Hardware and BIOS and firmware updates are managed by the Avaya Common Server team in conjunction with application R&D teams.

These servers must NOT be updated with BIOS or firmware updates from the vendor's web site.

Only Avaya provided updates can be used. Updating directly from the vendor's web site will result in an unsupported configuration.

You should **always** utilize the Avaya certified, bundled release. Do NOT upgrade individual components. This ensures that components interoperate in the manner in which they have been tested.

Resolution

Acquiring Update Tool

The ASP 100 Series Dell® R640 BIOS/Firmware update DVD is to be burned from the ISO file (R640fw-v13.0.iso) available from plds.avaya.com via PLDS Download ID: **ASP000000020.**

Download the **R640fw-v13.0.iso** to your PC and burn the image to a DVD. Ensure that the checksum of the downloaded image matches what is posted on PLDS. Burning the ISO as an image will create a bootable DVD disc.
Read through all steps below before inserting and running the BIOS/Firmware update disc that you have created.
It is always best practice to perform a complete backup of the system before any firmware or hardware maintenance.

Depending on the server's physical components and current firmware versions this procedure may take up to 60 minutes to complete.

After executing the procedures, the following components will be updated to the versions contained on the v13.0 disc.

ASP 100 Series Dell® R640 BIOS/Firmware update tool (v13.0) disc contains the following.
Rows highlighted in blue note an <u>update over the previous v12.0 version</u> introduced in PSN027106u.

Table 1: ASP 100 Series Dell® R640 BIOS/Firmware v13.0

Device Information	Firmware package release name	Firmware Version
iDRAC9 with Lifecycle Controller	iDRAC-with-Lifecycle-Controller_Firmware_TNYR2_LN64_7.00.00.171_A00.BIN	7.00.00.171
R640 BIOS	BIOS_56TY1_LN64_2.20.1_01.BIN	2.20.1
PERC H730/H730P/H830 Mini/Adapter	SAS-RAID_Firmware_700GG_LN_25.5.9.0001_A17.BIN	25.5.9.0001
PERC H750 Adapter	SAS-RAID_Firmware_NCXX4_LN64_52.26.0-5179_A04.BIN	52.26.0-5179
Intel Gigabit 4P I350-t rNDC	Network_Firmware_1R0W0_LN_22.5.7_A00.BIN	22.5.7
Broadcom Gigabit Ethernet BCM 5720	Network_Firmware_4JJW6_LN64_22.71.3_02.BIN	22.71.3
Intel X710, XXV710, and XL710 adapters *(only for high end ASBCE server)*	Network_Firmware_TNXW1_LN_22.5.7_A00.BIN	22.5.7
CPLD firmware for PowerEdge R640	CPLD_Firmware_9N4DH_LN_1.0.6_A00.BIN	1.0.6
Dell SEP Firmware for 14G Servers	Firmware_VV85D_LN_4.35_A00_06.BIN	4.35
Dell 12Gb Expander Firmware for 14G Servers	Firmware_60K1J_LN_2.52_A00.BIN	2.52
HGST Cobra F 600GB HDD 12Gbps SAS 3.5 10K 512n HUC101860CSS200	SAS-Drive_Firmware_X4FMC_LN_FU45_A00.BIN	FU45
Firmware version FJ40 for	SAS-Drive_Firmware_8MDXT_LN_FJ40_A00.BIN	FJ40

HGST drives. Vendor model numbers HUC101830CSS204, HUC101812CSS204, and HUC101860CSS204		
Seagate Skybolt ServoBP 600GB HDD 12Gbps SAS 2.5 10K 512n	SAS-Drive_Firmware_9KWMD_LN64_SBW5_A00.BIN SAS-Drive_Firmware_MXR36_LN64_SBW4_A00.BIN	SBW4/5
Firmware version ST36/37 for Seagate drives. Vendor model numbers ST600MM0069 and ST1200MM0099	SAS-Drive_Firmware_C161G_LN64_ST37_A00.BIN SAS-Drive_Firmware_X81HN_LN64_ST36_A00.BIN	ST36/37
Firmware version EA05for Toshiba drives. Vendor model numbers AL14SEB030NY, AL14SEB060NY and AL14SEB120NY	SAS-Drive_Firmware_TGCJ8_LN_EA05_A00.BIN	EA05
Toshiba AL14SE Lite SAS12 3.5 10K 512n (NS PD) Model Number: AL14SEB060N	SAS-Drive_Firmware_66RK9_LN_DH02_A00.BIN	DH02
Firmware version BS05 for Seagate HDD Thunderbug 2.5 SAS12 10K 512n drive. Vendor model numbers: ST600MM0238 and ST300MM0078	SAS-Drive_Firmware_2R4CX_LN_BS05_A00.BIN	BS05
TOSHIBA AL15SE ISE 2.5 600GB SAS12 10K 512NModel Number: AL15SEB060NYVendor Number: HDEBL84DAB51	SAS-Drive_Firmware_0T1RG_LN_EF06_A00.BIN	EF06
Toshiba Phoenix M4 WI SSD ISE 400GB 2.5 SAS 12Gbps 512n Model	SAS-Drive_Firmware_1DJXX_LN_AS10_A00.BIN	AS10
OS COLLECTOR 6.0	Diagnostics_Application_0G1JH_LN64_6.0_A00_01.BIN	6.0
Dell Diagnostics to verify proper operation of the hardware. Enterprise UEFI Diagnostics	Diagnostics_Application_R30YT_LN64_4301A73_4301.74_01.BIN	4301A73
OS Driver Pack for PowerEdge 14G servers. This Driver Pack contains applicable storage, NIC, and video drivers to support OS installation using the Dell Lifecycle Controller	Drivers-for-OS-Deployment_Application_N2VGD_LN_23.08.05_A00.BIN	23.08.05
iDRAC Service Module (iSM)	Systems-	5.2.0.0

is a lightweight software service that better integrates operating system (OS) features with iDRAC and can be installed on Dell 14G or later generation of PowerEdge servers.	Management_Application_957H0_LN64_5.2.0.0_A00.BIN	
iDRAC Service Module (iSM) is a lightweight software service that better integrates operating system (OS) features with iDRAC and can be installed on Dell 14G or later generation of PowerEdge servers.	Systems-Management_Application_X42KF_LN64_5.2.0.0_A00.BIN	5.2.0.0
DELL System Update (DSU) is a software designed to facilitate the application of updates on various Dell systems.	Systems-Management_Application_RWVV0_LN64_2.0.2.0_A00.BIN	2.0.2.0

Gracefully shut down the server according to Application Procedures
It is always best practice to perform a complete backup of the system before any firmware or hardware maintenance.

Firmware Update Procedures
Versions in pictures in this document are for illustrative purposes only. Versions may differ based on latest available BIOS/FW package.
BIOS/FW update testing was performed from v12 to v13. Updates from older versions may require intermediate step upgrades. Therefore, it is imperative to maintain software currency for BIOS/FW.

1. A Monitor, USB keyboard and mouse will be required to run the update tool.
2. Open DVD tray at server power up, insert the firmware update disc and close tray. Server will boot from update disc.
3. A hardware boot screen will first appear – note that the BIOS version displayed may vary depending on when the server was originally shipped.

```
F2  = System Setup
F10 = Lifecycle Controller (Config          BIOS Version: 2.6.4
      iDRAC, Update FW, Install OS)         iDRAC IPV4:  135.9.
F11 = Boot Manager
F12 = PXE Boot
```

Initializing Firmware Interfaces...

4. By default, Dell Deployment Toolkit(DTK) will boot from DVD:


```
Dell Bootable ISO (UEFI Mode)
Media Check
Exit




          Use the ▲ and ▼ keys to change the selection.
          Press 'e' to edit the selected item, or 'c' for a command prompt.
      The selected entry will be started automatically in 3s.
```
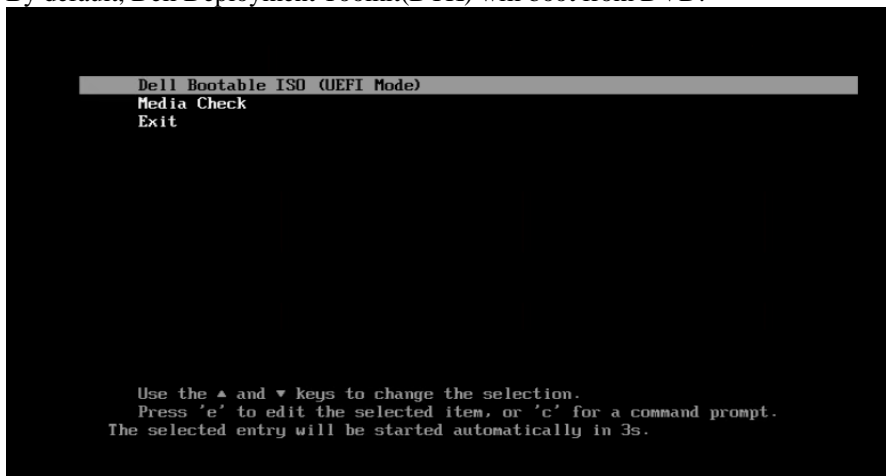
5. Booting the DTK can take up to 10 minutes. If the server does not boot from disc, verify that the disc is correctly inserted in the DVD drive (drive LED is intermittently active) and verify the media is burned correctly. Verify boot order has DVD drive before RAID controller. Once DTK has booted, an inventory of the server will be run to determine what packages should be installed. After inventory collection, DTK will begin updating eligible components that require an update. Package installation status is displayed. Ensure packages install successfully. Select <Enter> when all updates have run and the user is prompted to *Press Enter to reboot…* **Do not reboot the server until prompted.**

```
booting from cdrom with share_script as drm_files/apply_bundles.sh
mount /dev/cdrom /opt/dell/toolkit/systems
BUILD_NUMBER is matching ...
Valid DTK CD is found

Starting /run/initramfs/live/drm_files/apply_bundles.sh ....
warning: /opt/dell/toolkit/systems/RPMs/rhel7/yumrpms/dell-system-update-2.0.2.0-23.03.00.x86_64.rpm: Header V4 RSA/SHA512 S
ture, key ID 34d8786f: NOKEY
Preparing...                           ################################# [100%]
Updating / installing...
   1:dell-system-update-2.0.2.0-23.03.################################# [100%]
Installing dell-system-update ...
warning: /opt/dell/toolkit/systems/RPMs/dell-system-update-2.0.2.0-23.03.00.x86_64.rpm: Header V4 RSA/SHA512 Signature, key
4d8786f: NOKEY
DSU installation successful ...
Starting dsu for Avaya Firmware Update v13.0
DELL System Update 2.0.2.0
Copyright (C) 2014 -- 2023 DELL Proprietary.
Unable to read public file /usr/libexec/dell_dup/0x274E9C32857A9594.asc
Parsing configuration file...
Reading the catalog ...
Getting System Inventory ...
Determining Applicable Updates ...
Installing Drivers-for-OS-Deployment_Application_N2VGD_LN_23.08.05_A00
Installed successfully
Installing Systems-Management_Application_957H0_LN64_5.2.0.0_A00
Installed successfully
Installing Network_Firmware_4JJW6_LN64_22.71.3_02
 Installed successfully
Installing Network_Firmware_TNXW1_LN_22.5.7_A00
Installed successfully
Installing BIOS_56TY1_LN64_2.20.1_01
Installed successfully
Installing iDRAC-with-Lifecycle-Controller_Firmware_TNYR2_LN64_7.00.00.171_A00
l\lInstalled successfully
Please restart the system for successful update(s) to take effect
Done! Please run 'dsu --inventory' to check the inventory
Progress report is available at:/usr/libexec/dell_dup/DSU_STATUS.json
Exiting DSU!

drm_files/apply_bundles.sh execution is completed ....
Press Enter to reboot ...

_
```

6. If DTK runs, but no packages require updating, the following screen will be displayed with the message *No Applicable Update(s) Available*. Press <Enter> to reboot the server when prompted and check firmware versions. See section in this PSN on "Check Firmware Versions".


```
booting from cdrom with share_script as drm_files/apply_bundles.sh
mount /dev/cdrom /opt/dell/toolkit/systems
BUILD_NUMBER is matching ...
Valid DTK CD is found

Starting /run/initramfs/live/drm_files/apply_bundles.sh ....
warning: /opt/dell/toolkit/systems/RPMs/rhel7/yumrpms/dell-system-update-2.0.2.0-23.03.00.x86_64.rpm: Header V4 RSA/SHA512 Signature, key ID 34d8786f: NOKEY
Preparing...                           ################################# [100%]
Updating / installing...
   1:dell-system-update-2.0.2.0-23.03.################################# [100%]
Installing dell-system-update ...
warning: /opt/dell/toolkit/systems/RPMs/dell-system-update-2.0.2.0-23.03.00.x86_64.rpm: Header V4 RSA/SHA512 Signature, key ID 34d8786f: NOKEY
DSU installation successful ...
Starting dsu for Avaya Firmware Update v13.0
DELL System Update 2.0.2.0
Copyright (C) 2014 -- 2023 DELL Proprietary.
Unable to read public file /usr/libexec/dell_dup/0x274E9C32857A9594.asc
Parsing configuration file...
Reading the catalog ...
Getting System Inventory ...
Determining Applicable Updates
No Applicable Update(s) Available
Progress report is available at:/usr/libexec/dell_dup/DSU_STATUS.json
Exiting DSU!

drm_files/apply_bundles.sh execution is completed ....
Press Enter to reboot ...
```

7. If the DTK tool will not run, power-off server and remove power cord(s) for 1 minute. Re-insert power cords, power-up server and repeat firmware update process. Discharge the power button by holding it in for 15 seconds. Verify DVD media is in good condition and has been correctly burned. Verify boot order is set such that DVD drive is set before HDD. To verify boot order: when server is powering up select *<F2>System Setup/System BIOS/Boot Settings/Boot Sequence.* Verify Embedded SATA Port Optical Drive is first in boot order followed by the RAID Controller. Adjust the boot order and save if necessary following on the screen directions.

8. If the BIOS needed to be updated, **the new BIOS version is finalized AFTER the reboot.** After the reboot, the server will display the screen shown below. Note that the "Updating BIOS From" version will vary based on if the BIOS/FW has been kept current. In the example below, BIOS 2.13.3 is from the Avaya certified v10.1 BIOS/FW version. A similar screen would be seen for newer BIOS versions.
   a. DO NOT POWER DOWN THE SERVER.

b. WAIT for the BIOS update and any additional updates (CPLD) to complete.
   c. Server may reboot multiple times.
   d. **Do Not Power Down the server.**
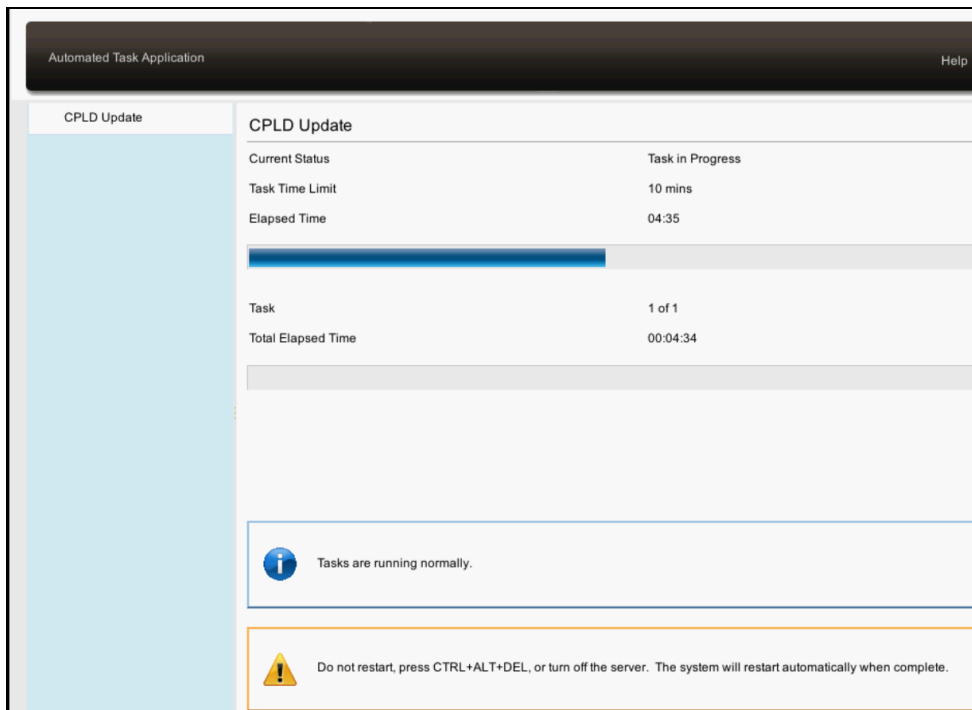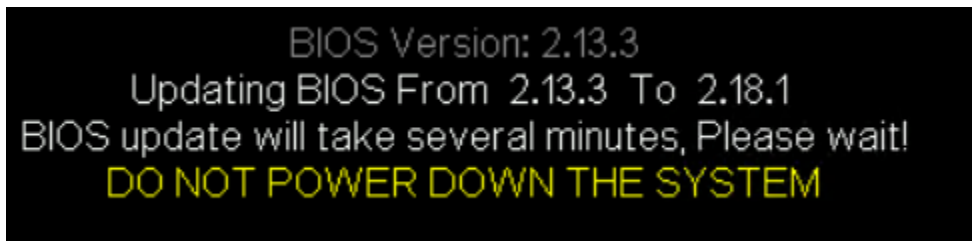
9. Once firmware updates are completed and finalized, **the DVD should be removed from the server** by pressing the eject button on the front of the DVD tray, otherwise the operating system (OS) will not boot and the DVD Firmware update disc will run again. Once the DVD is removed, the OS will begin to boot.
10. When the server starts to boot the OS, select <F10> to enter the Lifecycle Controller in order to verify the firmware updates. If the server has already booted the OS, or did not detect <F10>, simply reboot the server and select <F10> when prompted to verify the firmware updates.

11. If prompted, cancel out of the *Settings/Language and Keyboard* screen by pressing <esc>. Then select *Firmware Update → View Current Versions*:
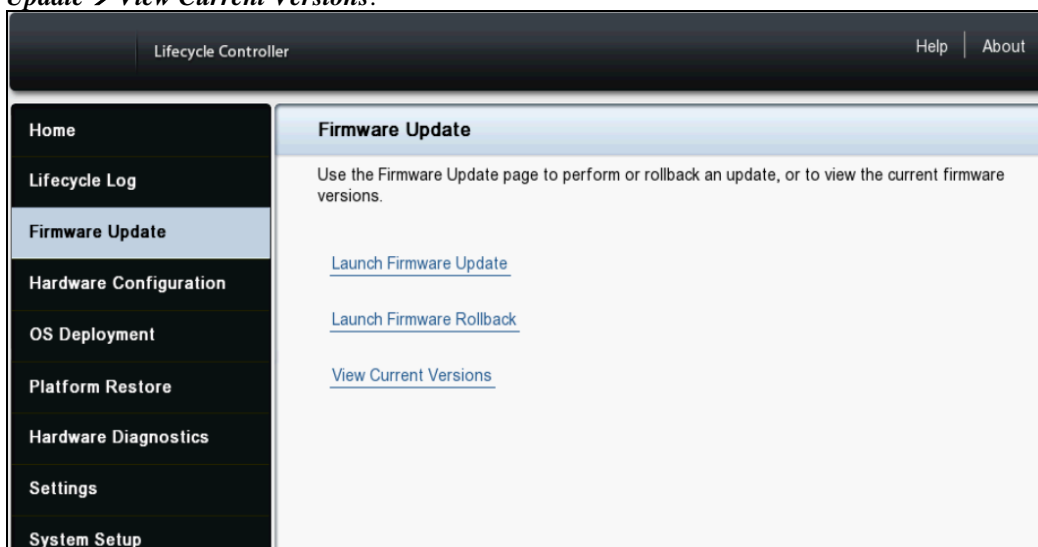
12. Verify versions as noted in **Table 1: ASP 100 Series Dell® R640 BIOS/Firmware v13.0** of this PSN. Ensure the following are updated to the versions listed in the table and confirm PERC packages remain as shown*: BIOS = 2.20.1, Broadcom Gigabit Ethernet = 22.71.3, Integrated Remote Access Controller (IDRAC) = 7.00.00.171, Lifecycle Controller = 7.00.00.00, Intel Gigabit 4P I350-t rNDC = 22.5.7 (Cascade Lake v1 server) and PERC H730P Mini = 25.5.9.0001 (Cascade Lake v1 server), PERC H750 Adapter = 52.26.0-5179 (Cascade Lake v2 server).*
Additional packages (i.e. OS Collector 14G, System CPLD, etc.) may update also depending on the vintage of server being updated.

Examples provided below for Cascade Lake v2 and Skylake and Cascade Lake v1 after updating to ASP 100 Series Dell® R640 Avaya Certified BIOS/Firmware v12.0.

Cascade Lake v2 Server type

(updated configuration with H750 RAID controller and 4x1GbE Broadcom Network Daughter Card):

Component Name	Version	Date and Time
BIOS	2.20.1	2024-03-18 22:15:00
Backplane 1	4.35	2021-12-07 18:54:46
Broadcom Gigabit Ethernet BCM5720 - 00:62:0B:5E:0F:40	22.71.3	2024-03-18 22:15:02
Broadcom Gigabit Ethernet BCM5720 - 00:62:0B:5E:0F:41	22.71.3	2024-03-18 22:15:03
Broadcom NetXtreme Gigabit Ethernet (BCM5720) - 34:73:5A:A0:0E:28	22.71.3	2024-03-18 22:15:01
Broadcom NetXtreme Gigabit Ethernet (BCM5720) - 34:73:5A:A0:0E:29	22.71.3	2024-03-18 22:15:01
Broadcom NetXtreme Gigabit Ethernet (BCM5720) - 34:73:5A:A0:0E:2A	22.71.3	2024-03-18 22:14:59
Broadcom NetXtreme Gigabit Ethernet (BCM5720) - 34:73:5A:A0:0E:2B	22.71.3	2024-03-18 22:15:00
Dell 64 Bit uEFI Diagnostics, version 4301, 4301A73, 4301.74	4301A73	2023-07-26 00:01:41
Dell OS Driver Pack, 23.08.05, A00	23.08.05	2024-03-18 21:33:58
Dell iDRAC Service Module Embedded Package v5.2.0.0, A00	5.2.0.0	2024-03-18 21:37:10
Disk 0 in Backplane 1 of RAID Controller in Slot 1	ST37	2023-07-26 00:22:38
Disk 1 in Backplane 1 of RAID Controller in Slot 1	ST37	2023-07-26 00:22:38
Disk 2 in Backplane 1 of RAID Controller in Slot 1	ST37	2023-07-26 00:22:38
Identity Module(FX4KG)	3.00	2022-02-08 00:26:28
Integrated Remote Access Controller	7.00.00.171	2024-03-18 21:50:59
Lifecycle Controller	7.00.00.171	2024-03-18 21:51:07
OS COLLECTOR, v6.0, A00	6.0	2022-02-08 00:26:27
PERC H750 Adapter	52.26.0-5179	2024-03-18 22:15:00
Power Supply.Slot.1	00.1B.53	2021-12-07 18:55:01
Power Supply.Slot.2	00.1B.53	2021-12-07 18:55:01
System CPLD	1.0.6	2022-02-08 00:26:28

Skylake and Cascade Lake v1 Server type

(original configuration with H730P RAID controller and 4x1GbE Intel Network Daughter Card):

13. After verifying the version information, select **Exit** in the upper right corner of the screen and then <YES> to reboot the server.

14. If a firmware package did not install, power-off the server and remove power cord(s) for 1 minute. Re-insert power cords, power-up server and repeat firmware update process.

Workaround or alternative remediation
N/A.
Remarks
April 29, 2024: Issue 1 – Initial publication.

Patch Notes

Backup before applying the patch	
Always.	
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
N/A.
Avaya Security Vulnerability Classification
N/A.
Mitigation
N/A.

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.