Product Support Notice

PSN #	PSN027086u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.

Original publication date: 08-Oct-19. This is Issue #01, published date: 08-Oct-19.	Severity/risk level	Medium	Urgency	When convenient	
Name of problem	PSN027086u – Avaya Common Server R3 Dell® R630 v5.1 BIOS/FW update including L1TF Vulnerability mitigation				

Products affected

Common Server R3 (Dell® R630)

Problem description

Dell release notes specific to this BIOS update state that they address the security vulnerability CVE-2018-3639 and CVE-2018-3640 requirements and also update the E5-2600 Product Family Processor Microcode versions.
In addition to the Intel Microcode BIOS updates, this package also includes updates to iDRAC8, Lifecycle Controller, RAID Controller, Ethernet NIC Firmware, HDD firmware.

General Information for L1TF:

An industry-wide issue was found in the way many modern microprocessor designs have implemented speculative execution of instructions (a commonly used performance optimization). This latest speculative execution side channel cache timing vulnerability is called L1 Terminal Fault (L1TF). There are three varieties of L1TF that have been identified. Each variety of L1TF could potentially allow unauthorized disclosure of information residing in the L1 data cache, a small pool of memory within each processor core designed to store information about what the processor core is most likely to do next.
Please reference **PSN020369u** for information about mitigation of L1TF vulnerabilities for Avaya Aura® application software.

- In order to help mitigate the Speculative Execution Vulnerabilities, the processor manufacturers and operating system developers provide software patches to their products. These are patches to the processors, hypervisors, and operating systems that the Avaya solutions utilize (they are not patches applied to the Avaya developed components of the solutions).
- Once these patches are received by Avaya, they are tested with the applicable Avaya solutions to characterize any impact on the performance of the Avaya solutions. The objective of the testing is to reaffirm product/solution functionality and to observe the performance of the Avaya solutions in conjunction with the patches using typical operating parameters.
- Avaya is reliant on our suppliers to validate the effectiveness of their respective Speculative Execution Vulnerability patches.
- The customer should be aware that implementing these patches may result in performance degradation and that results may vary to some degree for each deployment. The customer is responsible for implementing the patches, and for the results obtained from such patches.

Resolution

Avaya is providing an Avaya certified update that addresses the L1TF vulnerabilities with the necessary Intel Microcode BIOS updates. The Avaya Aura® Appliance Virtualization Platform hypervisor also provides the Intel Microcode updates for L1TF as L1TF was addressed in AVP 7.1.3.2 and 8.0.1. Reference PSN027074u. This has the same effect as the L1TF updates included in this package. However, the BIOS version on the server (e.g., via smbiosDump) will not reflect the update if installed only from the hypervisor.

In addition to the Intel Microcode BIOS updates, this package also includes updates to iDRAC8, Lifecycle Controller, RAID Controller, Ethernet NIC Firmware, HDD firmware.

This firmware is customer installable.

NOTE:

- **Avaya OEM servers used in turnkey application offers must NOT 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. Avaya creates a tailored Dell update 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 for the Dell R630. This firmware update is provided as a bootable, off-line tool that will install new firmware onto the server. Depending on the server's physical components and current firmware versions, this procedure may take up to 60 minutes to complete.

Acquiring Update Tool

Download the following file:

R630-fw-v5_1.iso **via** PLDS download ID **CMCS0000023** and burn a **bootable** DVD from it.

After executing the procedures, the following components will be updated to the listed firmware versions.

The R630 Server Firmware update (v5.1) disc contains:

Device Information	Firmware package release	Firmware Version
iDRAC8 with Lifecycle Controller	iDRAC-with-Lifecycle-Controller_Firmware_F675Y_LN_2.60.60.60_A00.BIN	2.60.60.60
BIOS – **Intel Microcode**	BIOS_2JFRF_LN_2.8.0.BIN	2.8.0
Enterprise UEFI Diagnostics	Diagnostics_Application_NNPW9_LN_4239A36_4239.44.BIN	4239A36
5720 DP 1G ADAPTER 5720 QP rNDC 1G BASE-T Broadcom 5720 1Gb Quad Port KR Blade Network Daughter Card	Network_Firmware_R4HKW_LN_20.8.4.BIN	20.8.4
PERC H730/H730P/H830 Mini/Adapter	SAS-RAID_Firmware_F675Y_LN_25.5.5.0005_A13.BIN	25.5.5.0005
13G PowerEdge Server Backplane Expander Firmware	Firmware_HYPYY_LN_3.35_A00-00.BIN	3.35
Valkyrie BP Valkyrie BP	SAS-Drive_Firmware_4CXN5_LN_VS0B_A00.BIN	4CXN5
2.5in SAS HDD	SAS-Drive_Firmware_8FF65_LN_LS0C_A00.BIN	8FF65
Seagate Kestrel 300GB HDD SAS 12Gbps 2.5" 15K 512nModel No: ST300MP0026Vendor PN: 1UT230-150 Seagate Kestrel 600GB HDD SAS 12Gbps 2.5" 15K 512nModel No: ST600MP0036Vendor PN: 1UU230-150 Seagate Kestrel 900GB HDD SAS 12Gbps 2.5" 15K 512nModel No: ST900MP0026Vendor PN: 1UV230-150	SAS-Drive_Firmware_37RKK_LN_KT37_A00.BIN	37RKK
Seagate Savvio 15K.3 146GB SAS 15K RPM Seagate Savvio 15K.3 300GB	SAS-Drive_Firmware_57G3N_LN_YS0C_A08.BIN	57G3N

SAS 15K RPM		
Seagate Thunderbug 300GB 2.5 SAS12 10K 512nModel No: ST300MM0078Vendor PN: 2C6230-150 Seagate Thunderbug 600GB 2.5 SAS12 10K 512nModel No: ST600MM0238Vendor PN: 2C7230-150	SAS-Drive_Firmware_64GYN_LN_BS04_A00.BIN	64GYN
2.5in SAS HDD	SAS-Drive_Firmware_68NGY_LN_LS0B_A00.BIN	68NGY
King Cobra F King Cobra F	SAS-Drive_Firmware_95VW1_LN_EA01_A00.BIN	95VW1
2.5in SAS HDD	SAS-Drive_Firmware_C407W_LN_VS0A_A00.BIN	C407W
Western Digital (SL305M) SAS 300GB 10K RPM Western Digital (SL305M) SAS 600GB 10K RPM Western Digital (SL305M) SAS 900GB 10K RPM	SAS-Drive_Firmware_G1XC6_LN_D1P3_A00.BIN	G1XC6
Seagate Kestrel FIPS-140 900GB HDD SAS 12Gbps 2.5" 15K 512nModel No: ST900MP0126Vendor PN: 1UV220-251	SAS-Drive_Firmware_G5W35_LN_KSC6_A00.BIN	G5W35
2.5in SAS HDD	SAS-Drive_Firmware_HKD9N_LN_DF0B_A00.BIN	HKD9N
Toshiba AL14SE-Lite 1200GB HDD 12Gbps SAS 2.5 10K 512n ISEModel No: AL14SEB120NYRegulatory Model No: AL14SEB120NYVendor PN: HDEBF81DAB51 Toshiba AL14SE-Lite 300GB HDD 12Gbps SAS 2.5 10K 512n ISEModel No: AL14SEB030NYRegulatory Model No: AL14SEB030NYVendor PN: HDEBF85DAB51 Toshiba AL14SE-Lite 600GB HDD 12Gbps SAS 2.5 10K 512n ISEModel No: AL14SEB060NYRegulatory Model No: AL14SEB060NYVendor PN: HDEBF83DAB51	SAS-Drive_Firmware_KHNKV_LN_EA02_A00.BIN	KHNKV
SEAGATE THUNDERBOLT 2.5 1.2TB 10K SAS12 512N SEAGATE THUNDERBOLT 2.5 300GB 10K SAS12 512N SEAGATE THUNDERBOLT 2.5 600GB 10K SAS12 512N	SAS-Drive_Firmware_KKNKX_LN_TT31_A00.BIN	KKNKX
2.5in SAS HDD	SAS-Drive_Firmware_M05PG_LN_KT35_A00.BIN	M05PG
2.5in SAS HDD	SAS-Drive_Firmware_M7J7F_LN_EA02_A00.BIN	M7J7F
AL13SE AL13SE AL13SE	SAS-Drive_Firmware_MCM30_LN_DE11_A00.BIN	MCM30

TOSHIBA AL13SE Lite 1.2 TB 2.5 12Gb 10K 512n SAS HDD Drive TOSHIBA AL13SE Lite 2.5 12Gb 10K 512n SAS HDD Drive TOSHIBA AL13SE Lite 2.5 12Gb 10K 512n SAS HDD Drive TOSHIBA AL14SE Lite 2.5 12Gb 10K 512n SAS HDD Drive	SAS-Drive_Firmware_NK8T7_LN_DM06_A00.BIN	NK8T7
Valkyrie BP Valkyrie BP	SAS-Drive_Firmware_RHYJY_LN_VT33_A00.BIN	RHYJY
HITACHI COBRA F 2.5 1.2TB 10K SAS12 512n HITACHI COBRA F 2.5 300GB 10K SAS12 512n HITACHI COBRA F 2.5 600GB 10K SAS12 512n	SAS-Drive_Firmware_VCW7P_LN_FJ34_A00.BIN	VCW7P

BIOS/Firmware Update Procedures

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.

Process Summary

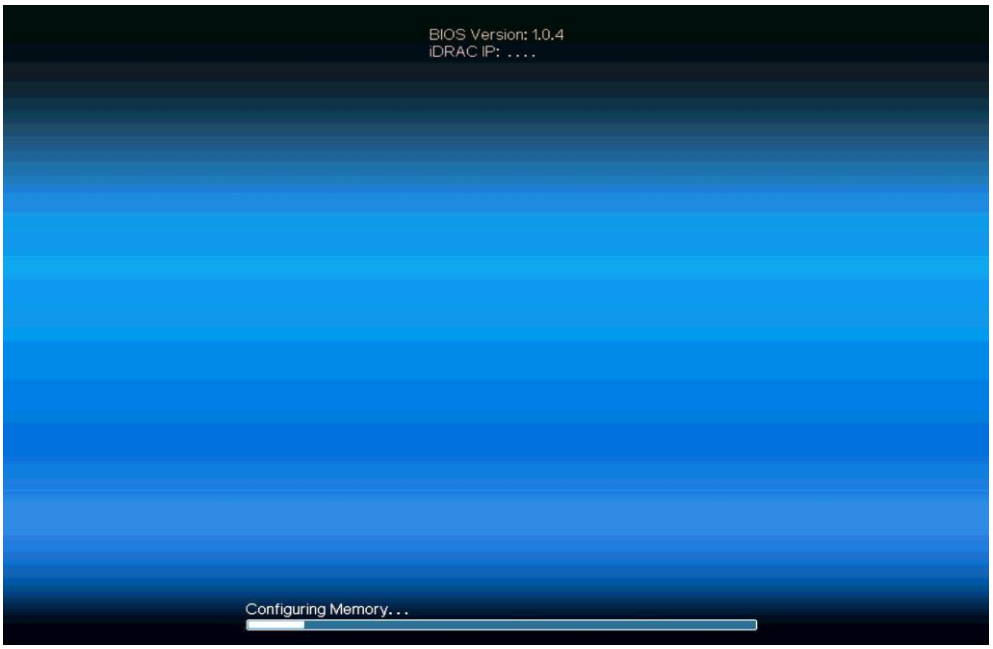
1. Perform a complete backup of the system.
2. Gracefully shutdown the server according to Application Procedures
3. Boot from Dell Diagnostics LiveCD
4. Insert media containing Dell Firmware Updates and Mount media
5. Run Installation Scripts
6. Check Results

Preparation

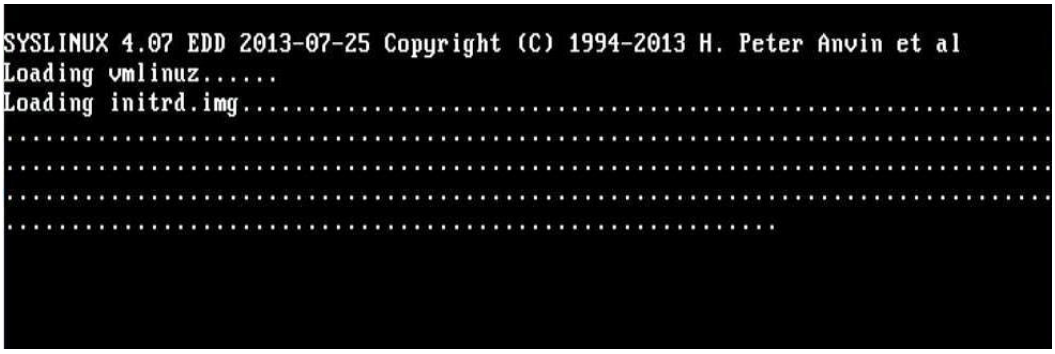
1. Backup the system.
2. Gracefully shut down the server according to Application Procedures
3. A monitor, USB keyboard and mouse will be required to run the update tool.
4. One blank CD/DVDs required for creating Update Media CD/DVD.
5. Download a copy of the firmware update (***R630-fw-v5_1.iso)*** via PLDS download ID **CMCS0000023** and burn a **bootable** CD/DVD from it.

Update Instructions

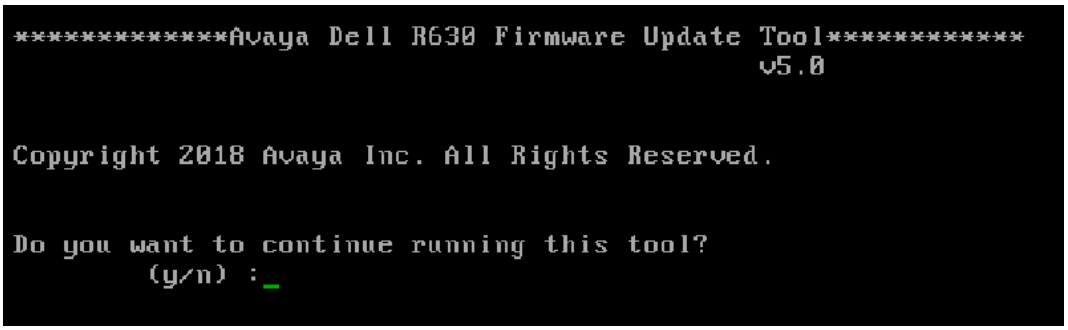
1. Insert the bootable media into the server and reboot or power up. A hardware boot screen will first appear.



2. The tool should boot from the DVD drive and the screen below indicates it is loading. This will take approximately 7-8 minutes to load.



3. Type **y <ENTER>** to run the firmware update. No more user interaction is required. Do NOT power off the server, reboot, reset or attempt any other activities on the server during the upgrade process. The Diagnostics update will install first. You may see USB connect and disconnect messages briefly. This is normal.



4. Some firmware packages may not update if the current version is equivalent (depends on what previous version was installed) and not all packages are applicable. For example, many HDD firmware packages are included but will only run if the corresponding HDD is detected.

```
PERC H730 Mini Controller 0

The version of this Update Package is the same as the currently installed versio
n.
Software application name: PERC H730 Mini Controller 0 Firmware
Package version: 25.5.4.0006
Installed version: 25.5.4.0006
```

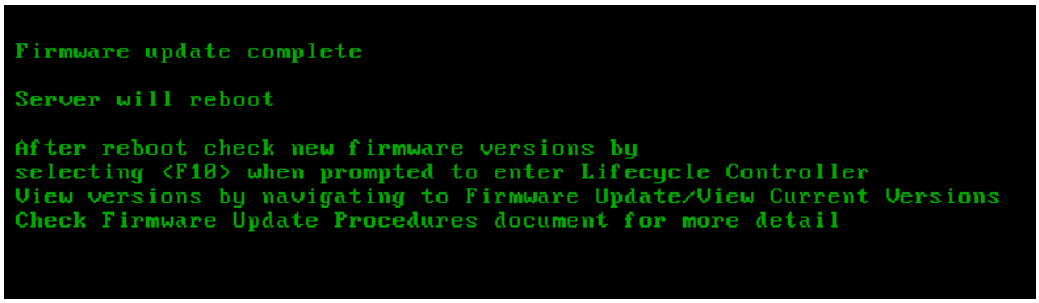
5. Not all packages are applicable and will not run if hardware device is not detected. Many HDD firmware packages are included but will only run if corresponding HDD is detected.

```
This Update Package is not compatible with your system configuration.

[8/25] - Executing SAS-Drive_Firmware_57G3N_LN_YS0C_A08.BIN
Collecting inventory...
Running validation...

This Update Package is not compatible with your system configuration.

[9/25] - Executing SAS-Drive_Firmware_64GYN_LN_BS04_A00.BIN
Collecting inventory...
Running validation...

This Update Package is not compatible with your system configuration.
```

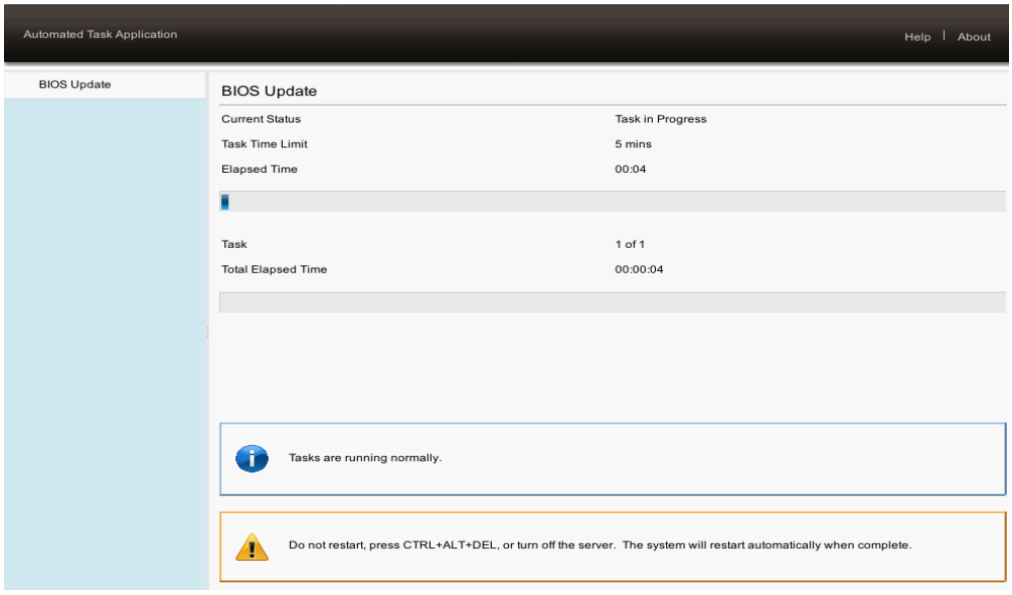
6. iDRAC/Lifecycle Controller and BIOS updates will run last.

```
THESE ACTIONS MAY CAUSE YOUR SYSTEM TO BECOME UNSTABLE!
The update completed successfully.
[25/25] - Executing BIOS_2JFRF_LN_2.8.0.BIN
Collecting inventory...
Running validation...

PowerEdge BIOS

The version of this Update Package is newer than the currently installed version
.
Software application name: BIOS
Package version: 2.8.0
Installed version: 2.7.1


Executing update...
WARNING: DO NOT STOP THIS PROCESS OR INSTALL OTHER PRODUCTS WHILE UPDATE IS IN P
ROGRESS.
THESE ACTIONS MAY CAUSE YOUR SYSTEM TO BECOME UNSTABLE!WARNING: DO NOT STOP THIS
 PROCESS OR
INSTALL OTHER PRODUCTS WHILE UPDATE IS IN PROGRESS.
THESE ACTIONS MAY CAUSE YOUR SYSTEM TO BECOME UNSTABLE!
.
The system should be restarted for the update to take effect.
```

7. Once the firmware update is complete, the server will reboot. Remove the disc when it is ejected.



8. After the server reboots, the system may automatically enter the Lifecycle Controller to finalize the firmware installation. You may see a BIOS configuration screen. Do not interrupt, restart, reset or turn off the server during this process. One to two auto-reboots may occur to finalize all firmware and recalibrate thermal parameters.

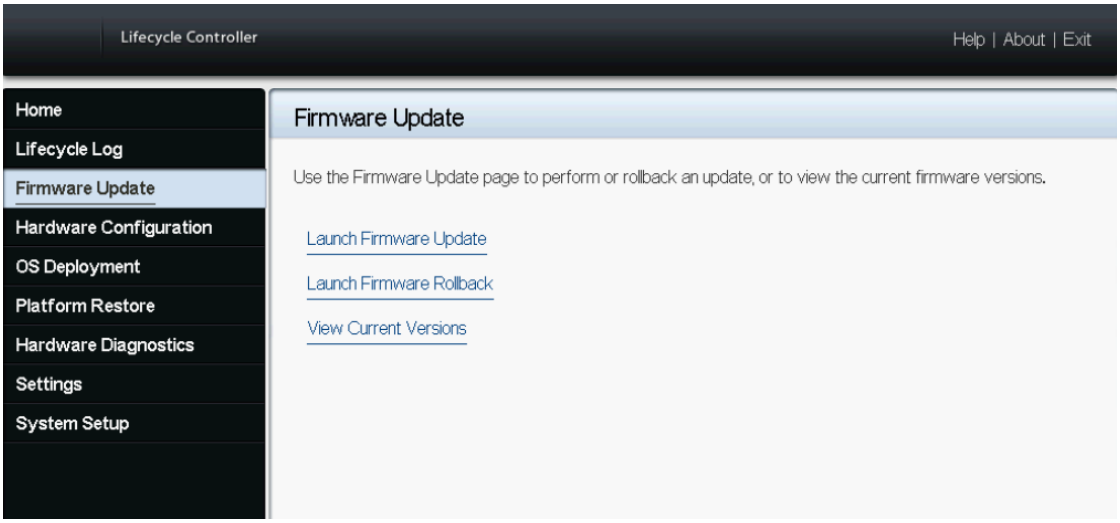


How to check firmware versions on a Dell R630.

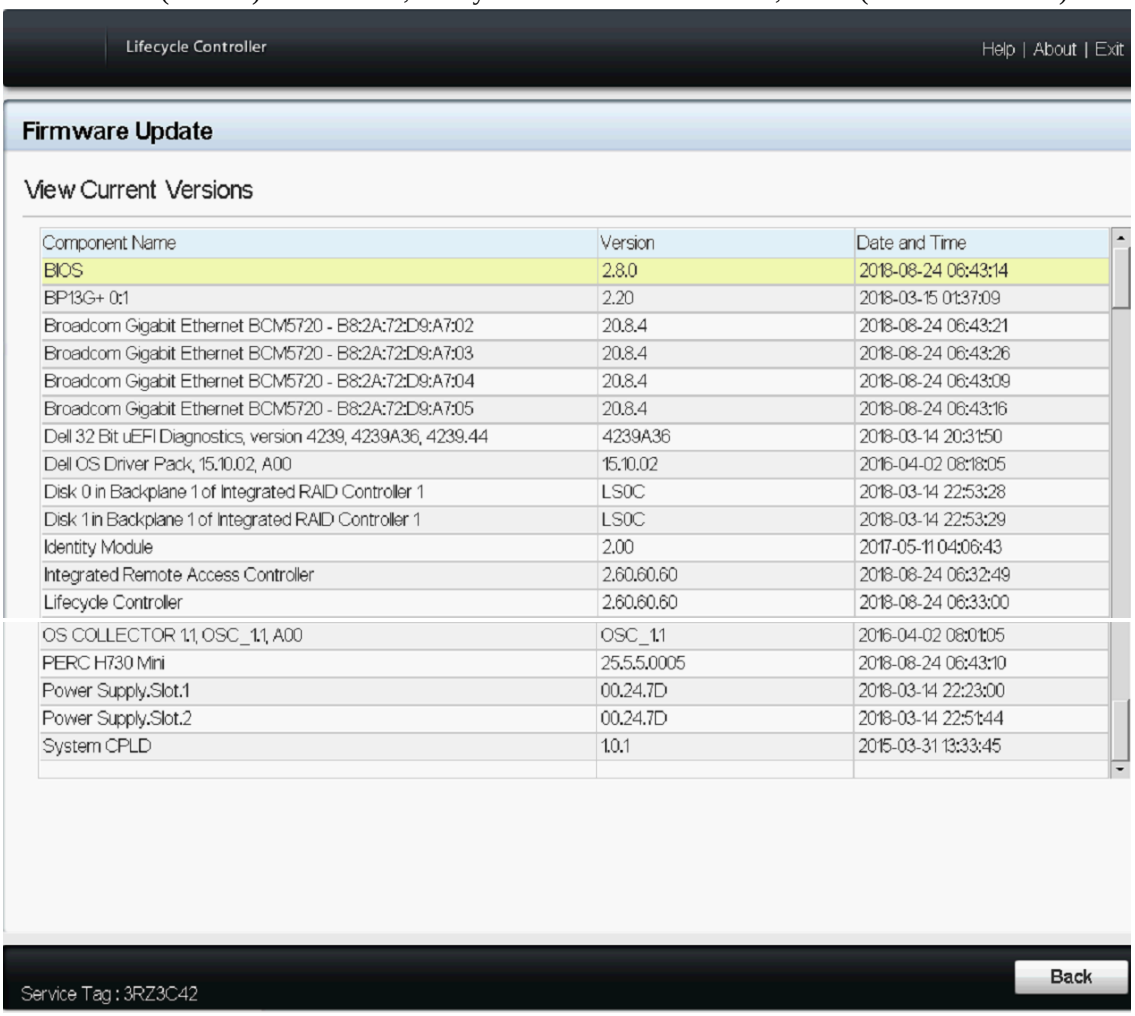
Requires monitor, USB keyboard and mouse.

1. Boot the server and during the first Hardware boot screen select <F10> for Lifecycle Controller.

2. Cancel out of the Settings/Language and Keyboard screen by pressing “esc” if necessary. Select **Firmware Update/View Current Versions** when the Lifecycle Controller Menu displays.



3. Verify Versions: BIOS = 2.8.0, Broadcom Gigabit Ethernet = 20.8.4 or greater, Integrated Remote Access Controller(IDRAC) = 2.60.60.60, Lifecycle Controller = 2.60.60.60, RAID (PERC H730 Mini) = 25.5.5.0005.



4. Select Exit in upper right corner of screen to reboot server.

If a firmware package did not install, power-off 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
October 08, 2019 – Issue 1.

Patch Notes

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

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

L1TF:

Vulnerability	CVSSv3 Base Score	CVSSv3 Metrics
CVE-2018-3615	6.4 (Medium)	CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:N
CVE-2018-3620	5.6 (Medium)	CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N
CVE-2018-3646	5.6 (Medium)	CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N
CVE-2018-3639	5.5 (Medium)	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
CVE-2018-3640	5.6 (Medium)	CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N

Spectre/Meltdown:

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

High for L1TF, Medium for Spectre/Meltdown.

Mitigation

N/A.

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