

PSN # PSN005139u

Original publication date: 12 March 2018. This is Issue #01, published date: 12-Mar-2018

Severity/risk level

High

Urgency

Immediately

Name of problem

IP Office & IP Office Contact Center Dell R230 Server vulnerability and System hang Memory Initialization Error - BIOS Firmware Update

Products affected

IP Office Dell R230 Servers:

390081 - R230 XL SERVER IP OFFICE UNIFIED COMMUNICATIONS

390082 - R230 XL SERVER IP OFFICE FRANCE TELECOM

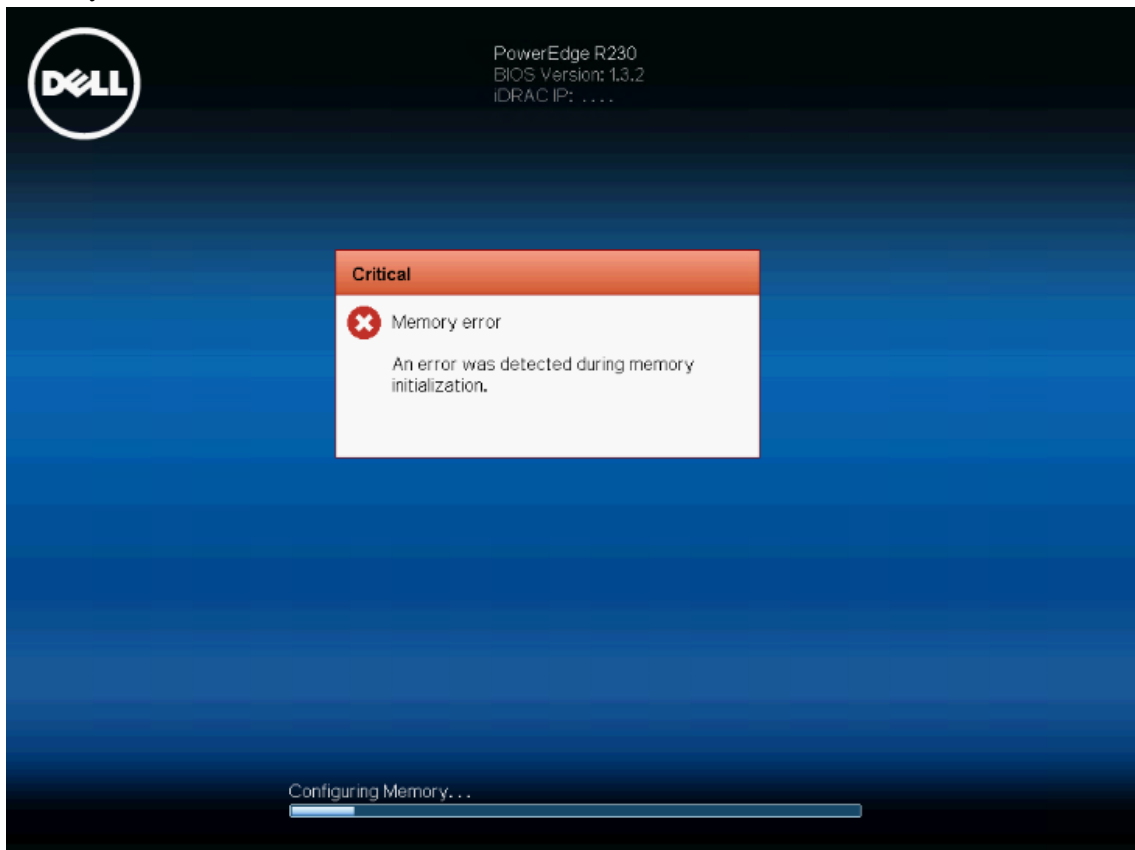
IP Office Contact Center Dell R230 Server

390083 - R230 XL SERVER IP OFFICE CONTACT CENTRE

Problem description

Intel has identified three security vulnerabilities in the BIOS firmware used to support the Intel Xeon E3-1200 v5 series processor. This processor family is used on the Dell R230 platforms sold by Avaya. Two of the fixes are related to the issues found in the Intel Management Engine and Trusted Execution Engine (CVE-2017-5706, CVE-2017-5709). The third fix includes the new Intel Microcode that is part of the solution for the Spectre Exploit (CVE-2017-5715).

This BIOS also includes the fix for the error message “PST0129 Memory is detected, but is not configurable. Check memory devices.”



The following is a link to the Dell Release Notes:

https://downloads.dell.com/FOLDER04798448M/1/R330_BIOS_2.4.3_ReleaseNotes.pdf

The following are links to the three vulnerabilities addressed by the BIOS update:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5706>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5709>

<https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5715>

The following is a link to the Dell Knowledge Base description of the system hang symptom:

<https://www.dell.com/support/article/us/en/19/sln303868/system-hangs-during-warm-reboot-at-critical-memory-initialization-error-for-poweredge-t130-r230-r330-and-t330-servers?lang=en>

Resolution

Dell has released the following BIOS version 2.4.3 to resolve the issue.

The EFI will be used to update all R230 servers and is available for download on Avaya Support portal in PLDS

This procedure is service interrupting and requires a system restart. Please plan accordingly.

A monitor, keyboard and mouse directly connected to the server are needed to perform this procedure.

Upgrade Instructions

File Format:Hard-Drive

File Name: R330-020403.efi

Download Type: HTTP

File Size: 6 MB

MD5:45b52f65fa39c1cc0e2b4ae982fc64ef

SHA1:47c981db0643236d0b0928c37d36075c88ed60c2

SHA-256:019fafc037294c831e5434a73ffe958cc256773245b689e43d9ae6a8275ceb1d

IP Office and IPOCC Installation Instructions:

Using a Windows PC:

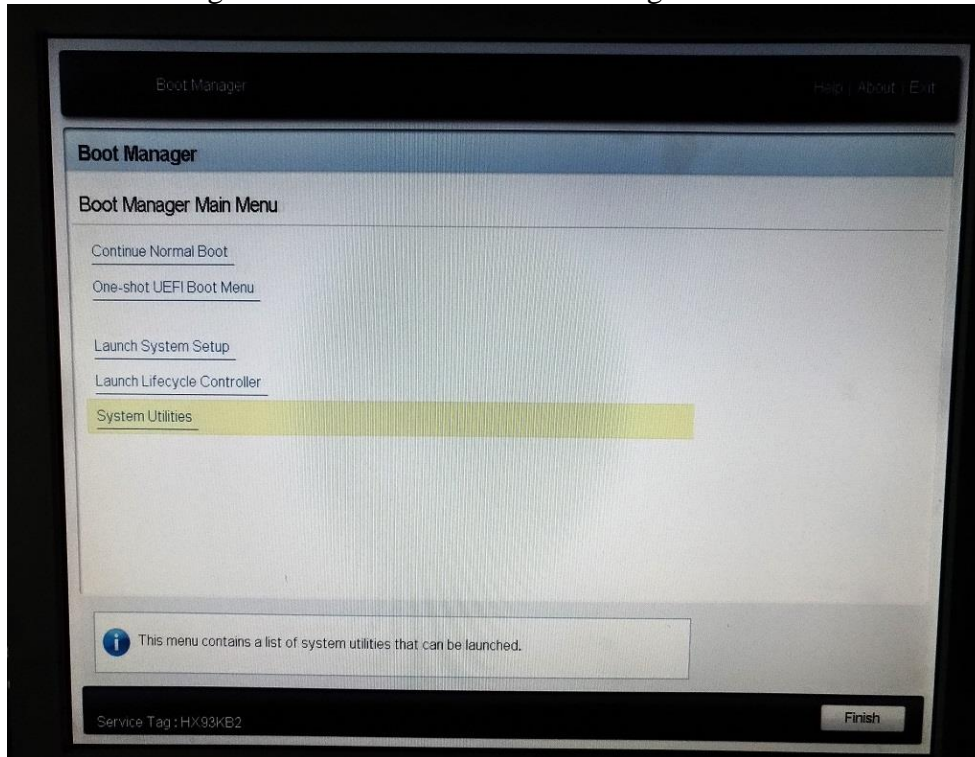
1. Download the R330-020403.efi file from PLDS.
2. Copy the file to a USB device that has been formatted with FAT32.
3. Plug in the USB device to the USB port on the front of the server.
4. **Shutdown the IPO 10.x.x Server.**
 - a. Log in to the server's web configuration pages.
 - b. Select the System page.
 - c. Click **Shutdown**. The menu prompts you to confirm the action.
 - d. Click **Yes** to confirm that you want to proceed with the shutdown.

The login page appears again. Do not attempt to log in again immediately.

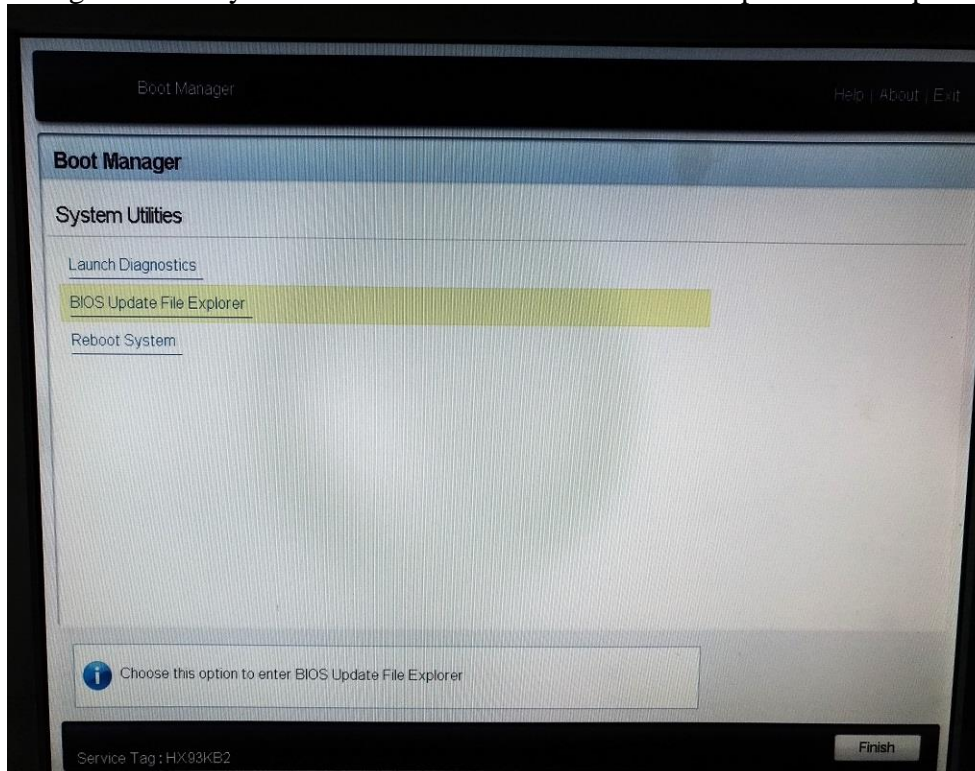
After a few minutes, typically no more than 2 minutes, the server shuts down.

5. **Shutdown the IPOCC Server.**

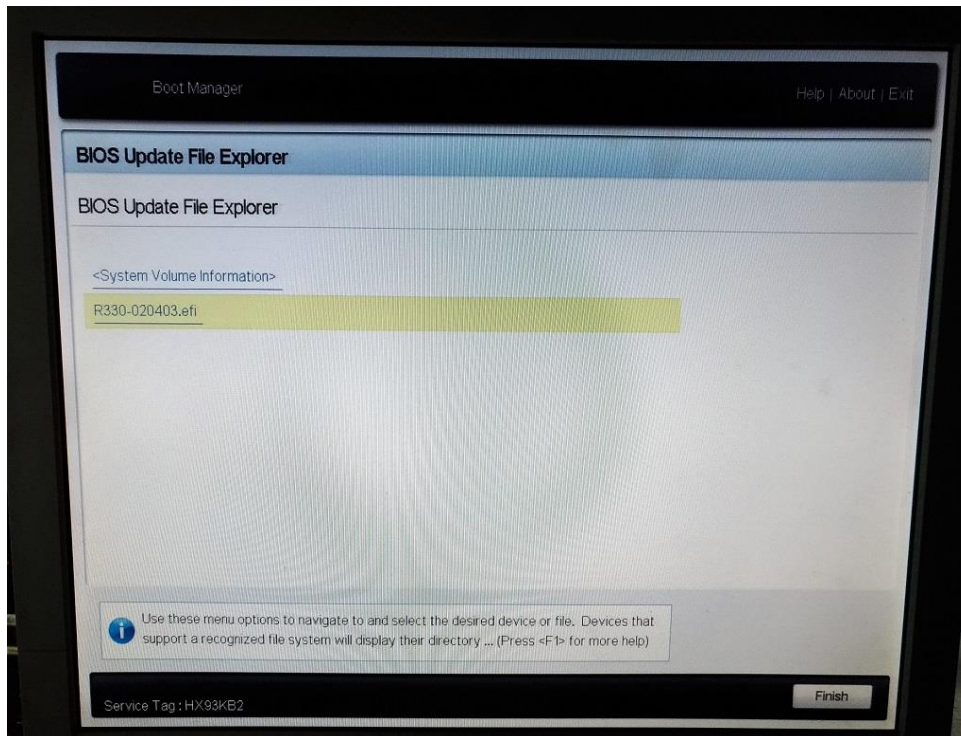
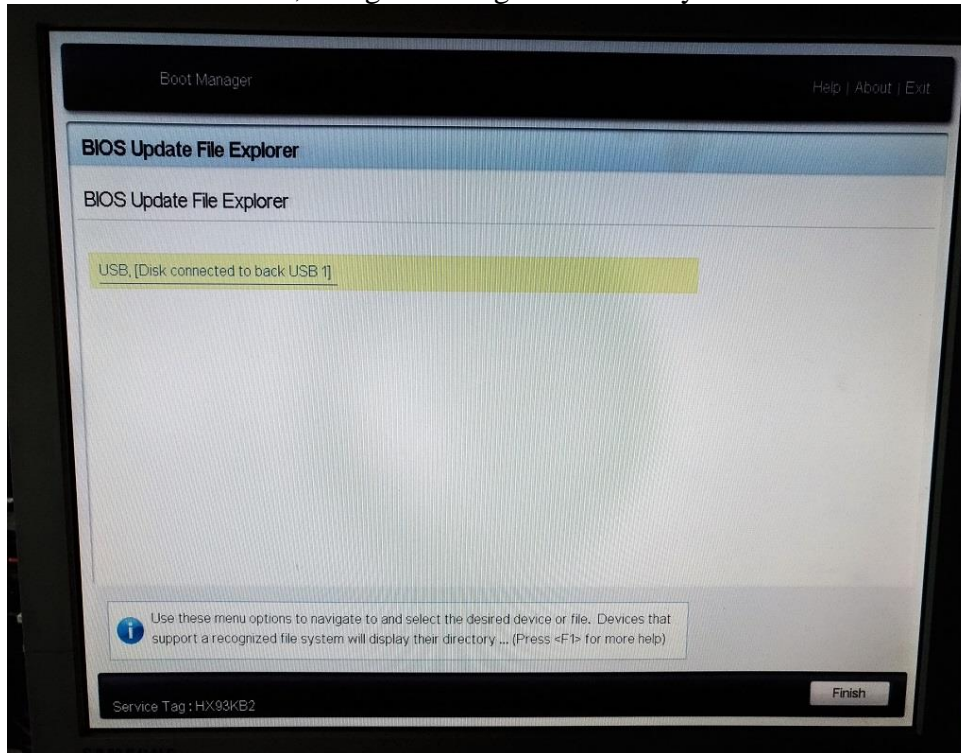
- a. Log in to the IPOCC server.
 - b. Select the Windows Start Menu.
 - c. Select **Shutdown**.
6. Press the power button to restart the server.
7. Press F11 during POST to enter BIOS Boot Manager.



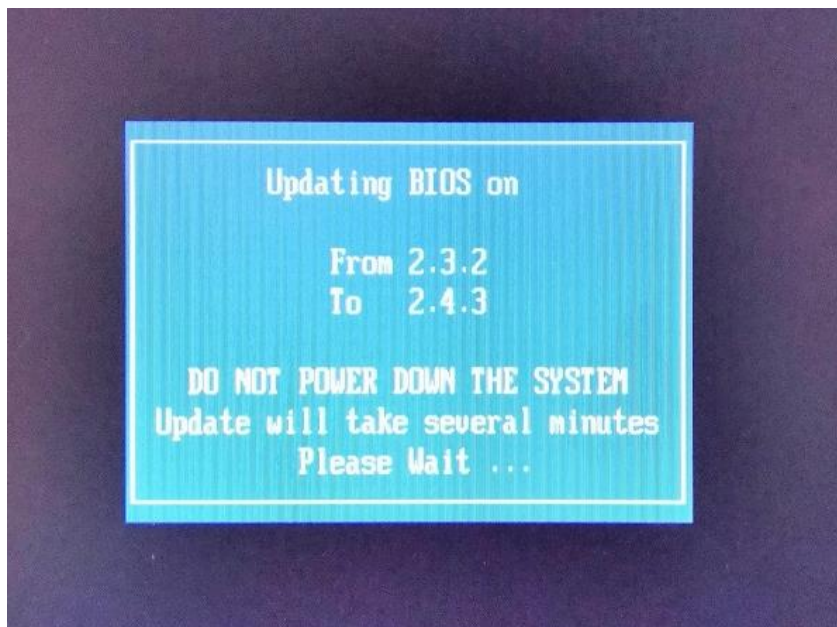
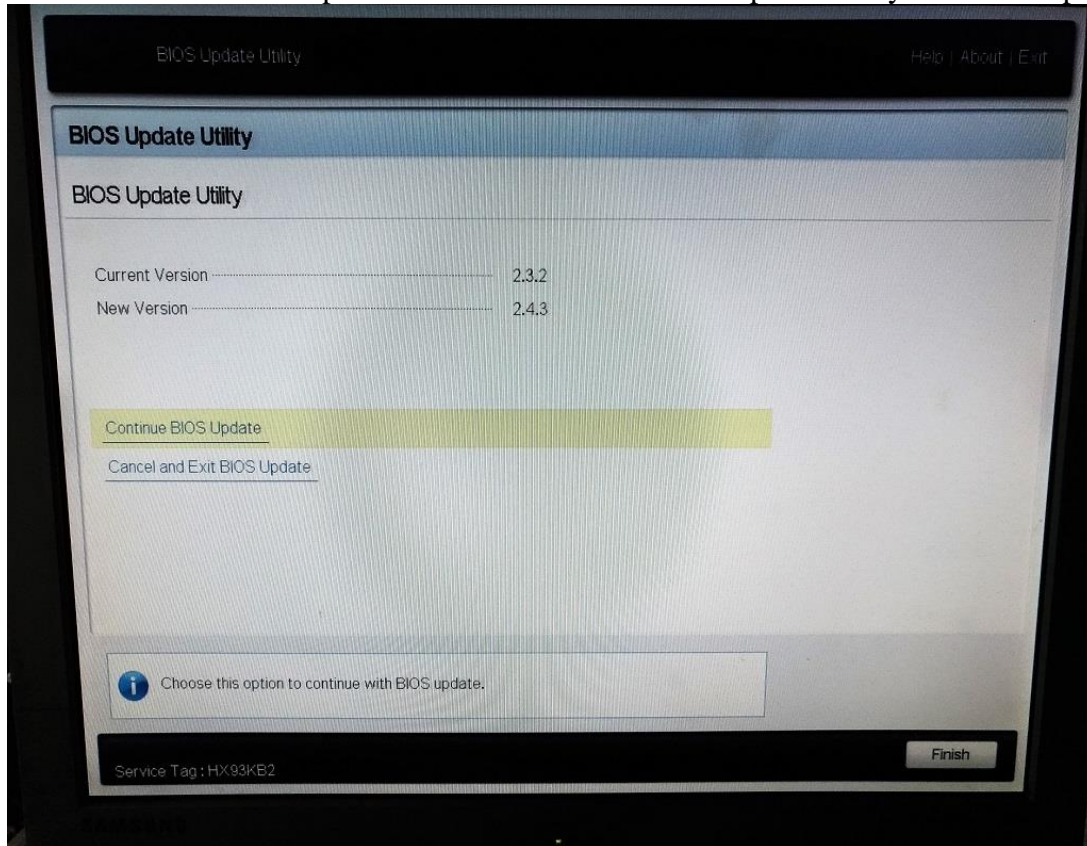
8. Navigate to the System Utilities menu and select BIOS Update File Explorer.



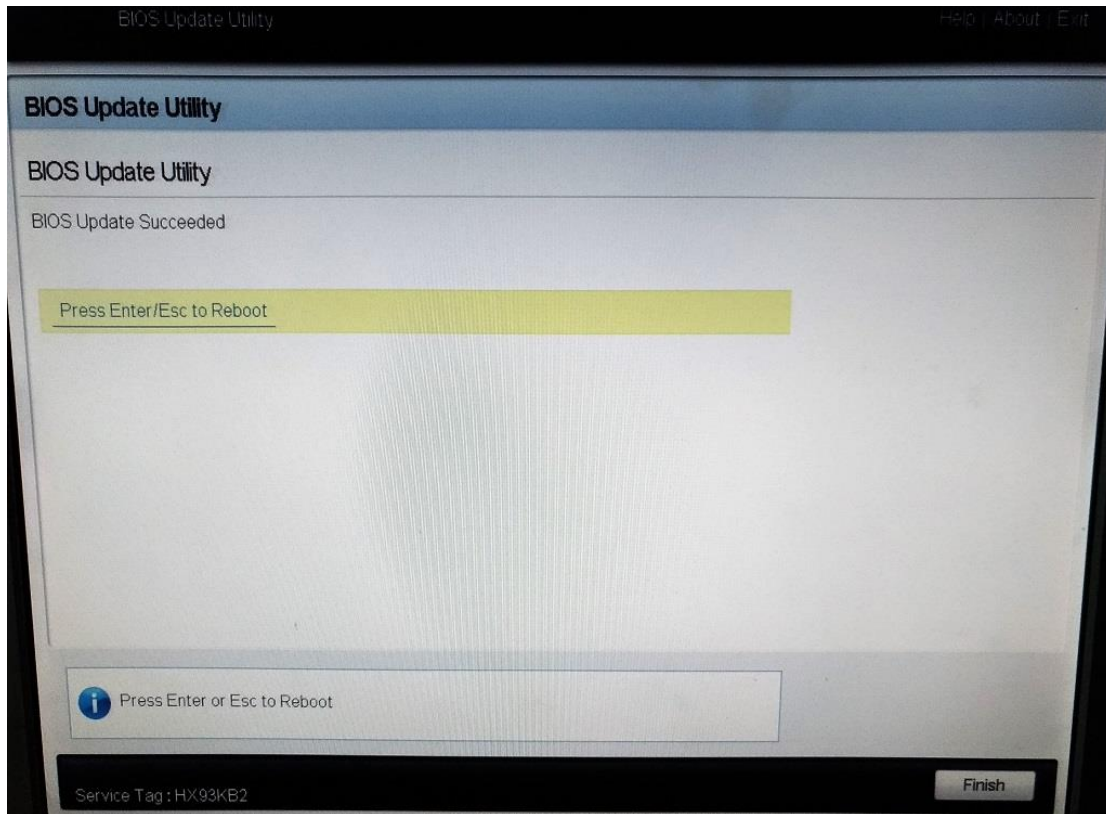
9. Select the USB device, navigate through the directory contents and select the executable (.efi).



10. Select Continue BIOS Update and follow the instructions provided by the BIOS Update utility.

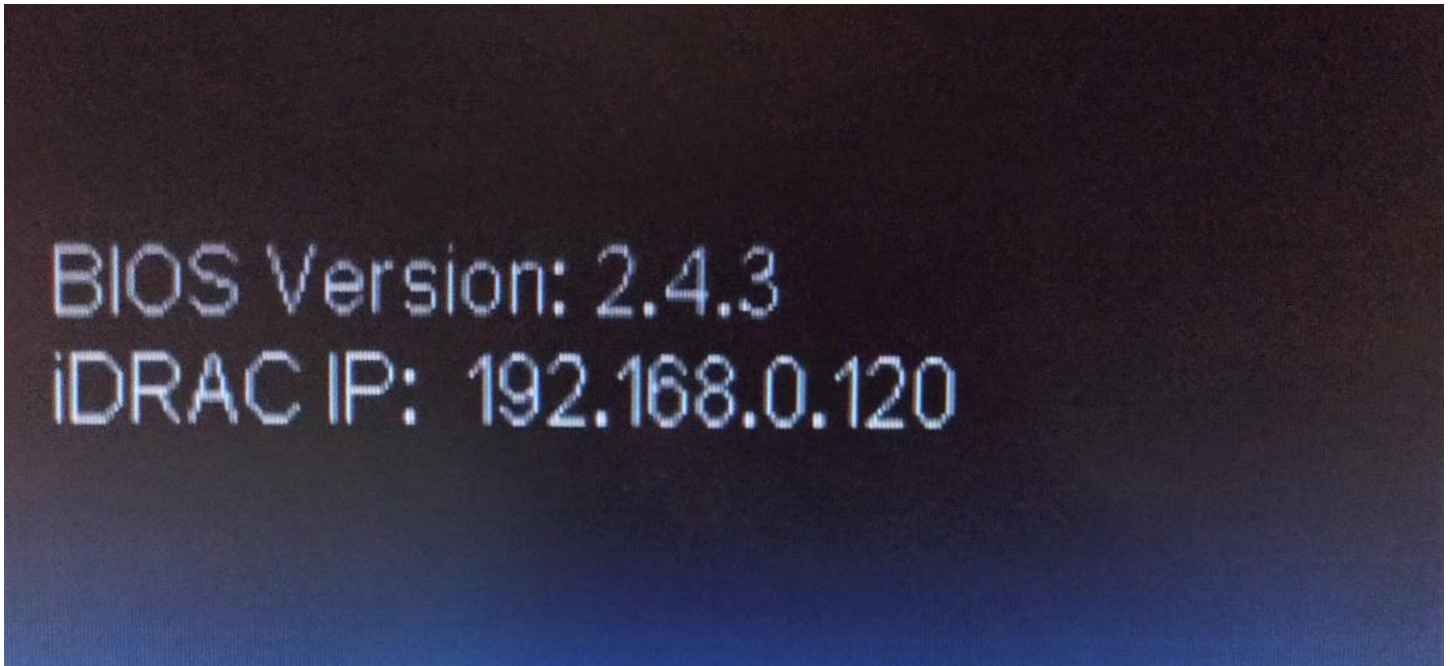


11. Follow the instructions to reboot the server.



BIOS Verification Steps

After the BIOS has been successfully upgraded, observe the BIOS version displayed on the system console during the restart.



Workaround or alternative remediation

N/A

Remarks

Avaya has completed testing on both the IP Office & IPOCC Dell R230 servers. No issues were found and the upgrades to the BIOS went smoothly. It is recommended that customers apply this update as soon as possible.

Dell has cut over production of the new BIOS on all new orders provided to Avaya as of March 5, 2018.

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

No

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

This PSN specifically addresses a security risk in the Dell Server BIOS as described in the following Dell notice:

<http://www.dell.com/support/home/us/en/19/drivers/driversdetails?driverId=WDY2P>

Avaya Security Vulnerability Classification

Medium

Mitigation

Upgrade BIOS as soon as possible.

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.