BIOS Version 1.3.7 for Dell EMC PowerEdge Servers: R740, R740XD, R640, and R940.

And for Dell Precision 7920 Rack workstation

Release Notes

Release Notes

BIOS

Basic Input / Output System (BIOS) facilitate the hardware initialization process and transition control to the operating system.

Current Version

1.3.7

Release Date

February 2018

Previous Version

1.2.71 (demoted)

Importance

URGENT: Dell highly recommends applying this update as soon as possible. The update contains changes to improve the reliability and availability of your Dell system.

Platform(s) affected

The PowerEdge R740, R740XD, R640, and R940 servers. Also, for the Precision 7920 Rack workstation.

What's New

- Added NVDIMM-N Namespace support for the VMWare ESXi 6.7 version.
- Updated the Intel Trusted Execution Technology (Intel TXT) BIOS Authenticated Code Module (ACM) to version 1.3.4.
- Updated the Intel Processor and Memory Reference Code to PLR3.1.
- To address CVE-2017-5715 (http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5715):
  - o   Updated the Intel Xeon Processor Scalable Family Processor Microcode to version 0x43.
  - o   CVE-2017-5753 and CVE-2017-5754 are addressed by the Operating System & Hypervisor updates.
  - o   For more information, visit http://www.dell.com/support/article/SLN308588.

  Note: For the PowerEdge R940 servers only: Added instantaneous OCP adjustment for system configuration register values of Voltage System Agent (VSA).

Fixes

- BIOS takes a long time to handle correctable memory errors.
- For certain PCIe slots, manual slot bifurcation may not work.
- PCIe fatal error may be reported when a particular Network Daughter Card (NDC) is installed.
- Rarely, the system may stop at POST (Power-On-Self-Test) when running reboot test in the BIOS boot mode.
- Several NVMe-related defects.
- Resolved an Intel Management Engine related issue that caused the BIOS version update to fail (fails only when the server is kept turned on continuously for 24 days since the previous AC power cycle). See the **Important notes** section in this Release Notes.

Important notes

- This release provides continued code optimization to improve stability and performance.
- An Intel Management Engine related issue that caused the BIOS update to fail is resolved in this BIOS 1.3.7 version.
  - This included remedy becomes effective only after the device is updated with this BIOS 1.3.7 version.

    Warning: Running an iDRAC RACADM power cycle command while running an operating system causes an ungraceful shutdown.
  - To work around this issue, AC power cycle the system or run the iDRAC RACADM power cycle command before updating the BIOS.
  - The first attempt to upgrade to this 1.3.7 version will fail, but the second attempt will pass if done within 24 days after the first attempt.
  - For more information about this issue and safely working around this issue, see:
    - Dell EMC PSQN SLN 309027 here: http://www.dell.com/support/article/us/en/04/SLN309027.
    - Intel HSD125807 here:

      https://www.intel.com/content/dam/www/program/design/us/en/documents/hsd125807-hmrfpo-timeout-ta-337128.pdf?asset=16254.

_____

History of previous Release Notes

Version

1.2.71 (demoted)

Release Date

December 2017

What's New

- Enhancement to address CVE-2017-5715 (http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5715) and details to be published in January 2018.
- Updated the Intel Xeon Processor Scalable Family Processor Microcode to version 0x3A.

Fixes

None for this release.

_____

Version

1.2.11

Release Date

October 2017

What's New

- Added support for updating the NVDIMM-N firmware version.

- Updated the Intel Trusted Execution Technology (Intel TXT) BIOS Authenticated Code Module (ACM) to version 1.3.3.
- Updated the Intel Processor and Memory Reference Code to PLR2.
- Updated the Intel Xeon Processor Scalable Family Processor Microcode to version 0x2C.
- C States default is changed to Disabled in the Performance System Profile.

Fixes

- Mitigated the security vulnerability CVE-2017-5706 (http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5706). Details anticipated to be published in November 20, 2017.
- Mitigated the security vulnerability CVE-2017-5709 (http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5709). Details anticipated to be published in November 20, 2017.

_____