BIOS Version 1.4.5 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

1.4.5

Release Date

April 2018

Previous Version

1.3.7

Importance

RECOMMENDED: Dell EMC recommends applying this update during your next scheduled update cycle. The update contains feature enhancements or changes that will help keep your system software current and compatible with other system modules (firmware, BIOS, drivers, and software).

Platform(s) affected

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

What's New

- Added a check to prevent BIOS downgrade when 18nm DIMMs are installed in 2 DPC (DIMMs per Channel) configuration and memory frequency is 2666 Mhz or higher. For more information, visit http://www.dell.com/support/article/SLN309212.
- Added support for HDD and USB placeholders in UEFI Boot Sequence.
- Added UEFI Capsule Firmware (BIOS only) Update Support by using O/S update service such as Windows update. This feature is available only for Precision 7920 Rack workstations.
- Log NVDIMM-N erase failure to SEL (System Event Log).

  Note: This error is already logged to Lifecycle Controller log.
- Added capability to re-enable a disabled PCIe clock after a warm reboot.
- Added enhancements to UEFI BIOS update tool. Users cannot use UEFI BIOS update utilities to downgrade BIOS to earlier version once the 1.4.5 or later BIOS version is installed on the system.

  Note: Update Package can still be used to downgrade BIOS to versions earlier than 1.4.5.
- Updated the Intel Trusted Execution Technology (Intel TXT) BIOS Authenticated Code Module (ACM) to version 1.3.5.
- Updated the Intel Processor and Memory Reference Code to PLR5.

Fixes

- An unsuccessful NVDIMM-N firmware update may be reported as successful.
- TPM region is not reserved in the E820 table.

- When specific 4-core CPUs are installed, the system stops responding during the NVDIMM-N firmware update operation.
- Updated the IP4 stack to support point-to-point link with the 31-bit mask.
- Able to set 'System Password' in HII when the 'System Lockdown Mode' is enabled.

Important notes

This release provides continued code optimization to improve stability and performance.

History of previous Release Notes

Version

1.3.7

Release Date

February 2018

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):
  - Updated the Intel Xeon Processor Scalable Family Processor Microcode to version 0x43.
  - CVE-2017-5753 and CVE-2017-5754 are addressed by the Operating System & Hypervisor updates.
  - 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.

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.
