## VMware Deliverable Release Notes

This document does not apply to HPE Superdome servers. For information on HPE Superdome , see the following links:

HPE Integrity Superdome X
HPE Superdome Flex

Information on HPE Synergy supported VMware ESXi OS releases, HPE ESXi Custom Images and HPE Synergy Custom SPPs is available at:

VMware OS Support Tool for HPE Synergy

Information on HPE Synergy Software Releases is available at:

HPE Synergy Software Releases - Overview

## VMware Upgrade Pack 1.3.1 for VMware ESXi 7.0 Release Notes


BIOS (Login Required) - System ROM
Driver - Lights-Out Management
Driver - Network
Driver - System Management
Firmware - Network
Firmware - NVDIMM
Firmware - Storage Controller
Firmware - Storage Fibre Channel
Software - Management
Software - System Management


### BIOS (Login Required) - System ROM Top

ROM Flash Firmware Package - HPE Apollo 2000 Gen10/HPE ProLiant XL170r/XL190r Gen10 (U38) Servers
Version: 2.40_10-26-2020 **(Recommended)**
Filename: U38_2.40_10_26_2020.fwpkg

**Important Note!**

**Important Notes:**

This version of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2020.2 guidance.

**Deliverable Name:**

HPE Apollo 2000 Gen10/ProLiant XL170r/XL190r Gen10 System ROM - U38

**Release Version:**

2.40_10-26-2020

**Last Recommended or Critical Revision:**

2.40_10-26-2020

**Previous Revision:**

2.36_07-16-2020

**Firmware Dependencies:**

None

**Enhancements/New Features:**

Added a new BIOS/Platform Configuration (RBSU) option to Memory Options called Refresh Watermarks. When selecting the Low Watermark setting, the memory controller will help reduce susceptibility to a DDR4 RowHammer attack. It is expected that a memory performance impact will be seen when enabling the Low Watermark setting. The default operation of the system has not changed and customers wanting to provide additional RowHammer protection should enable this setting.

Added support to BIOS/Platform Configuration (RBSU) to allow importing and exporting Secure Boot signature lists as a signed binary file. This is useful to import the Microsoft revocation list binary file into the Secure Boot DBX as found on the UEFI forum at https://uefi.org/revocationlistfile.

Updated the System ROM to allow for an increased amount of 64-bit Memory Mapped I/O available for third party options cards.

Updated the System ROM support for One Button Secure Erase functionality with the latest HPE option devices.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

**Problems Fixed:**

This version of the system ROM includes updates to the Intel Memory Reference Code which may help improve memory stability for systems configured with two DIMMs per channel. Please consult Intel sighting documentation for more details on the improvements included in the Intel IPU.2.2020 release. This issue is not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigations for security vulnerabilities documented as CVE-2020-8696. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-0381. The Intel microcode patches included in this release are version 0x02006A08 (CPUID 50654), 0x04003003 (CPUID 50656) and 0x05003003 (CPUID 50567). These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS advisories and security vulnerabilities documented as CVE-2020-0587, CVE-2020-0588, CVE-2020-0590, CVE-2020-0591, CVE-2020-0592 and CVE-2020-0593. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00358. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS platform code advisories and security vulnerabilities documented as CVE-2020-8738, CVE-2020-8739, CVE-2020-8740, and CVE-2020-8764. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00390. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which addressed an issue where the system may get stuck in a reboot loop during memory training. This issue was introduced with the v2.30 System ROM. This issue was not unique to HPE servers.

Addressed an issue where the memory locality of the ACPI SLIT table was not being created properly. In rare cases, the incorrect ACPI SLIT values could cause unexpected impacts to system performance. This issue was introduced in the v2.10 version of the System ROM and was not seen with previous versions of the System ROM.

Addressed an issue where NVMe Hot-plug and Hot-add would not function properly with VMware. This issue did not impact NVMe Hot-plug or Hot-add with other operating systems.

Addressed an issue where the system would not properly call out a memory replacement event in the Integrated Management Log (IML) if an uncorrected memory failure occurred during an Advanced Double DRAM Device Correction (ADDDC) sparing operation. This fix only impacts the incorrect logging of these events and does not impact the normal operation of the system in terms of causing uncorrected memory failures or causing any change to the operation of A3DC functionality. This issue only impacts systems configured for fast Fault Tolerant Memory Mode (ADDDC).

Addressed an issue where the BIOS/Platform Configuration (RBSU) option for the Extended Memory Test could be automatically disabled after a system reboot. This issue was introduced with the v2.30 System ROM and was not seen with earlier version of the System ROM.

**Known Issues:**

None

**Fixes**

**Important Notes:**

This version of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2020.2 guidance.

**Firmware Dependencies:**

None

**Problems Fixed:**

This version of the system ROM includes updates to the Intel Memory Reference Code which may help improve memory stability for systems configured with two DIMMs per channel. Please consult Intel sighting documentation for more details on the improvements included in the Intel IPU.2.2020 release. This issue is not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigations for security vulnerabilities documented as CVE-2020-8696. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-0381. The Intel microcode patches included in this release are version 0x02006A08 (CPUID 50654), 0x04003003 (CPUID 50656) and 0x05003003 (CPUID 50567). These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS advisories and security vulnerabilities documented as CVE-2020-0587, CVE-2020-0588, CVE-2020-0590, CVE-2020-0591, CVE-2020-0592 and CVE-2020-0593. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00358. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS platform code advisories and security vulnerabilities documented as CVE-2020-8738, CVE-2020-8739, CVE-2020-8740, and CVE-2020-8764. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00390. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which addressed an issue where the system may get stuck in a reboot loop during memory training. This issue was introduced with the v2.30 System ROM. This issue was not unique to HPE servers.

Addressed an issue where the memory locality of the ACPI SLIT table was not being created properly. In rare cases, the incorrect ACPI SLIT values could cause unexpected impacts to system performance. This issue was introduced in the v2.10 version of the System ROM and was not seen with previous versions of the System ROM.

Addressed an issue where NVMe Hot-plug and Hot-add would not function properly with VMware. This issue did not impact NVMe Hot-plug or Hot-add with other operating systems.

Addressed an issue where the system would not properly call out a memory replacement event in the Integrated Management Log (IML) if an uncorrected memory failure occurred during an Advanced Double DRAM Device Correction (ADDDC) sparing operation. This fix only impacts the incorrect logging of these events and does not impact the normal operation of the system in terms of causing uncorrected memory failures or causing any change to the operation of A3DC functionality. This issue only impacts systems configured for fast Fault Tolerant Memory Mode (ADDDC).

Addressed an issue where the BIOS/Platform Configuration (RBSU) option for the Extended Memory Test could be automatically disabled after a system reboot. This issue was introduced with the v2.30 System ROM and was not seen with earlier version of the System ROM.

**Known Issues:**

None

**Enhancements**

Added a new BIOS/Platform Configuration (RBSU) option to Memory Options called Refresh Watermarks. When selecting the Low Watermark setting, the memory controller will help reduce susceptibility to a DDR4 RowHammer attack. It is expected that a memory performance impact will be seen when enabling the Low Watermark setting. The default operation of the system has not changed and customers wanting to provide additional RowHammer protection should enable this setting.

Added support to BIOS/Platform Configuration (RBSU) to allow importing and exporting Secure Boot signature lists as a signed binary file. This is useful to import the Microsoft revocation list binary file into the Secure Boot DBX as found on the UEFI forum at https://uefi.org/revocationlistfile.

Updated the System ROM to allow for an increased amount of 64-bit Memory Mapped I/O available for third party options cards.

Updated the System ROM support for One Button Secure Erase functionality with the latest HPE option devices.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

---

ROM Flash Firmware Package - HPE Apollo 4200 Gen10/HPE ProLiant XL420 Gen10 (U39) Servers
Version: 2.40_10-26-2020 **(Recommended)**
Filename: U39_2.40_10_26_2020.fwpkg

**Important Note!**

**Important Notes:**

This version of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2020.2 guidance.

**Deliverable Name:**

HPE Apollo 4200 Gen10/ProLiant XL420 Gen10 System ROM - U39

**Release Version:**

2.40_10-26-2020

**Last Recommended or Critical Revision:**

2.40_10-26-2020

**Previous Revision:**

2.36_07-16-2020

**Firmware Dependencies:**

None

**Enhancements/New Features:**

Added a new BIOS/Platform Configuration (RBSU) option to Memory Options called Refresh Watermarks. When selecting the Low Watermark setting, the memory controller will help reduce susceptibility to a DDR4 RowHammer attack. It is expected that a memory performance impact will be seen when enabling the Low Watermark setting. The default operation of the system has not changed and customers wanting to provide additional RowHammer protection should enable this setting.

Added support to BIOS/Platform Configuration (RBSU) to allow importing and exporting Secure Boot signature lists as a signed binary file. This is useful to import the Microsoft revocation list binary file into the Secure Boot DBX as found on the UEFI forum at https://uefi.org/revocationlistfile.

Updated the System ROM to allow for an increased amount of 64-bit Memory Mapped I/O available for third party options cards.

Updated the System ROM support for One Button Secure Erase functionality with the latest HPE option devices.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

**Problems Fixed:**

This version of the system ROM includes updates to the Intel Memory Reference Code which may help improve memory stability for systems configured with two DIMMs per channel. Please consult Intel sighting documentation for more details on the improvements included in the Intel IPU.2.2020 release. This issue is not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigations for security vulnerabilities documented as CVE-2020-8696. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-0381. The Intel microcode patches included in this release are version 0x02006A08 (CPUID 50654), 0x04003003 (CPUID 50656) and 0x05003003 (CPUID 50567). These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS advisories and security vulnerabilities documented as CVE-2020-0587, CVE-2020-0588, CVE-2020-0590, CVE-2020-0591, CVE-2020-0592 and CVE-2020-0593. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00358. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS platform code advisories and security vulnerabilities documented as CVE-2020-8738, CVE-2020-8739, CVE-2020-8740, and CVE-2020-8764. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00390. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which addressed an issue where the system may get stuck in a reboot loop during memory training. This issue was introduced with the v2.30 System ROM. This issue was not unique to HPE servers

Addressed an issue where the memory locality of the ACPI SLIT table was not being created properly. In rare cases, the incorrect ACPI SLIT values could cause unexpected impacts to system performance. This issue was introduced in the v2.10 version of the System ROM and was not seen with previous versions of the System ROM.

Addressed an issue where NVMe Hot-plug and Hot-add would not function properly with VMware. This issue did not impact NVMe Hot-plug or Hot-add with other operating systems.

Addressed an issue where the system would not properly call out a memory replacement event in the Integrated Management Log (IML) if an uncorrected memory failure occurred during an Advanced Double DRAM Device Correction (ADDDC) sparing operation. This fix only impacts the incorrect logging of these events and does not impact the normal operation of the system in terms of causing uncorrected memory failures or causing any change to the operation of A3DC functionality. This issue only impacts systems configured for fast Fault Tolerant Memory Mode (ADDDC).

Addressed an issue where the BIOS/Platform Configuration (RBSU) option for the Extended Memory Test could be automatically disabled after a system reboot. This issue was introduced with the v2.30 System ROM and was not seen with earlier version of the System ROM.

**Known Issues:**

None

## Fixes

**Important Notes:**

This version of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2020.2 guidance.

**Firmware Dependencies:**

None

**Problems Fixed:**

This version of the system ROM includes updates to the Intel Memory Reference Code which may help improve memory stability for systems configured with two DIMMs per channel. Please consult Intel sighting documentation for more details on the improvements included in the Intel IPU.2.2020 release. This issue is not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigations for security vulnerabilities documented as CVE-2020-8696. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-0381. The Intel microcode patches included in this release are version 0x02006A08 (CPUID 50654), 0x04003003 (CPUID 50656) and 0x05003003 (CPUID 50567). These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS advisories and security vulnerabilities documented as CVE-2020-0587, CVE-2020-0588, CVE-2020-0590, CVE-2020-0591, CVE-2020-0592 and CVE-2020-0593. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00358. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS platform code advisories and security vulnerabilities documented as CVE-2020-8738, CVE-2020-8739, CVE-2020-8740, and CVE-2020-8764. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00390. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which addressed an issue where the system may get stuck in a reboot loop during memory training. This issue was introduced with the v2.30 System ROM. This issue was not unique to HPE servers

Addressed an issue where the memory locality of the ACPI SLIT table was not being created properly. In rare cases, the incorrect ACPI SLIT values could cause unexpected impacts to system performance. This issue was introduced in the v2.10 version of the System ROM and was not seen with previous versions of the System ROM.

Addressed an issue where NVMe Hot-plug and Hot-add would not function properly with VMware. This issue did not impact NVMe Hot-plug or Hot-add with other operating systems.

Addressed an issue where the system would not properly call out a memory replacement event in the Integrated Management Log (IML) if an uncorrected memory failure occurred during an Advanced Double DRAM Device Correction (ADDDC) sparing operation. This fix only impacts the incorrect logging of these events and does not impact the normal operation of the system in terms of causing uncorrected memory failures or causing any change to the operation of A3DC functionality. This issue only impacts systems configured for fast Fault Tolerant Memory Mode (ADDDC).

Addressed an issue where the BIOS/Platform Configuration (RBSU) option for the Extended Memory Test could be automatically disabled after a system reboot. This issue was introduced with the v2.30 System ROM and was not seen with earlier version of the System ROM.

**Known Issues:**

None

## Enhancements

Added a new BIOS/Platform Configuration (RBSU) option to Memory Options called Refresh Watermarks. When selecting the Low Watermark setting, the memory controller will help reduce susceptibility to a DDR4 RowHammer attack. It is expected that a memory performance impact will be seen when enabling the Low Watermark setting. The default operation of the system has not changed and customers wanting to provide additional RowHammer protection should enable this setting.

Added support to BIOS/Platform Configuration (RBSU) to allow importing and exporting Secure Boot signature lists as a signed binary file. This is useful to import the Microsoft revocation list binary file into the Secure Boot DBX as found on the UEFI forum at https://uefi.org/revocationlistfile.

Updated the System ROM to allow for an increased amount of 64-bit Memory Mapped I/O available for third party options cards.

Updated the System ROM support for One Button Secure Erase functionality with the latest HPE option devices.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

ROM Flash Firmware Package - HPE Apollo 4510 Gen10/HPE ProLiant XL450 Gen10 (U40) Servers
Version: 2.40_10-26-2020 **(Recommended)**
Filename: U40_2.40_10_26_2020.fwpkg

**Important Note!**

**Important Notes:**

This version of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2020.2 guidance.

**Deliverable Name:**

HPE Apollo 4510 Gen10/ProLiant XL450 Gen10 System ROM - U40

**Release Version:**

2.40_10-26-2020

**Last Recommended or Critical Revision:**

2.40_10-26-2020

**Previous Revision:**

2.36_07-16-2020

**Firmware Dependencies:**

None

**Enhancements/New Features:**

Added a new BIOS/Platform Configuration (RBSU) option to Memory Options called Refresh Watermarks. When selecting the Low Watermark setting, the memory controller will help reduce susceptibility to a DDR4 RowHammer attack. It is expected that a memory performance impact will be seen when enabling the Low Watermark setting. The default operation of the system has not changed and customers wanting to provide additional RowHammer protection should enable this setting.

Added support to BIOS/Platform Configuration (RBSU) to allow importing and exporting Secure Boot signature lists as a signed binary file. This is useful to import the Microsoft revocation list binary file into the Secure Boot DBX as found on the UEFI forum at https://uefi.org/revocationlistfile.

Updated the System ROM to allow for an increased amount of 64-bit Memory Mapped I/O available for third party options cards.

Updated the System ROM support for One Button Secure Erase functionality with the latest HPE option devices.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

**Problems Fixed:**

This version of the system ROM includes updates to the Intel Memory Reference Code which may help improve memory stability for systems configured with two DIMMs per channel. Please consult Intel sighting documentation for more details on the improvements included in the Intel IPU.2.2020 release. This issue is not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigations for security vulnerabilities documented as CVE-2020-8696. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-0381. The Intel microcode patches included in this release are version 0x02006A08 (CPUID 50654), 0x04003003 (CPUID 50656) and 0x05003003 (CPUID 50567). These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS advisories and security vulnerabilities documented as CVE-2020-0587, CVE-2020-0588, CVE-2020-0590, CVE-2020-0591, CVE-2020-0592 and CVE-2020-0593. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00358. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS platform code advisories and security vulnerabilities documented as CVE-2020-8738, CVE-2020-8739, CVE-2020-8740, and CVE-2020-8764. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00390. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which addressed an issue where the system may get stuck in a reboot loop during memory training. This issue was introduced with the v2.30 System ROM. This issue was not unique to HPE servers

Addressed an issue where the memory locality of the ACPI SLIT table was not being created properly. In rare cases, the incorrect ACPI SLIT values could cause unexpected impacts to system performance. This issue was introduced in the v2.10 version of the System ROM and was not seen with previous versions of the System ROM.

Addressed an issue where NVMe Hot-plug and Hot-add would not function properly with VMware. This issue did not impact NVMe Hot-plug or Hot-add with other operating systems.

Addressed an issue where the system would not properly call out a memory replacement event in the Integrated Management Log (IML) if an uncorrected memory failure occurred during an Advanced Double DRAM Device Correction (ADDDC) sparing operation. This fix only impacts the incorrect logging of these events and does not impact the normal operation of the system in terms of causing uncorrected memory failures or causing any change to the operation of A3DC functionality. This issue only impacts systems configured for fast Fault Tolerant Memory Mode (ADDDC).

Addressed an issue where the BIOS/Platform Configuration (RBSU) option for the Extended Memory Test could be automatically disabled after a system reboot. This issue was introduced with the v2.30 System ROM and was not seen with earlier version of the System ROM.

**Known Issues:**

None

**Fixes**

**Important Notes:**

This version of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2020.2 guidance.

**Firmware Dependencies:**

None

**Problems Fixed:**

This version of the system ROM includes updates to the Intel Memory Reference Code which may help improve memory stability for systems configured with two DIMMs per channel. Please consult Intel sighting documentation for more details on the improvements included in the Intel IPU.2.2020 release. This issue is not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigations for security vulnerabilities documented as CVE-2020-8696. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-0381. The Intel microcode patches included in this release are version 0x02006A08 (CPUID 50654), 0x04003003 (CPUID 50656) and 0x05003003 (CPUID 50567). These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS advisories and security vulnerabilities documented as CVE-2020-0587, CVE-2020-0588, CVE-2020-0590, CVE-2020-0591, CVE-2020-0592 and CVE-2020-0593. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00358. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS platform code advisories and security vulnerabilities documented as CVE-2020-8738, CVE-2020-8739, CVE-2020-8740, and CVE-2020-8764. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00390. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which addressed an issue where the system may get stuck in a reboot loop during memory training. This issue was introduced with the v2.30 System ROM. This issue was not unique to HPE servers

Addressed an issue where the memory locality of the ACPI SLIT table was not being created properly. In rare cases, the incorrect ACPI SLIT values could cause unexpected impacts to system performance. This issue was introduced in the v2.10 version of the System ROM and was not seen with previous versions of the System ROM.

Addressed an issue where NVMe Hot-plug and Hot-add would not function properly with VMware. This issue did not impact NVMe Hot-plug or Hot-add with other operating systems.

Addressed an issue where the system would not properly call out a memory replacement event in the Integrated Management Log (IML) if an uncorrected memory failure occurred during an Advanced Double DRAM Device Correction (ADDDC) sparing operation. This fix only impacts the incorrect logging of these events and does not impact the normal operation of the system in terms of causing uncorrected memory failures or causing any change to the operation of A3DC functionality. This issue only impacts systems configured for fast Fault Tolerant Memory Mode (ADDDC).

Addressed an issue where the BIOS/Platform Configuration (RBSU) option for the Extended Memory Test could be automatically disabled after a system reboot. This issue was introduced with the v2.30 System ROM and was not seen with earlier version of the System ROM.

**Known Issues:**

None

**Enhancements**

Added a new BIOS/Platform Configuration (RBSU) option to Memory Options called Refresh Watermarks. When selecting the Low Watermark setting, the memory controller will help reduce susceptibility to a DDR4 RowHammer attack. It is expected that a memory performance impact will be seen when enabling the Low Watermark setting. The default operation of the system has not changed and customers wanting to provide additional RowHammer protection should enable this setting.

Added support to BIOS/Platform Configuration (RBSU) to allow importing and exporting Secure Boot signature lists as a signed binary file. This is useful to import the Microsoft revocation list binary file into the Secure Boot DBX as found on the UEFI forum at https://uefi.org/revocationlistfile.

Updated the System ROM to allow for an increased amount of 64-bit Memory Mapped I/O available for third party options cards.

Updated the System ROM support for One Button Secure Erase functionality with the latest HPE option devices.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

---

ROM Flash Firmware Package - HPE ProLiant BL460c Gen10 (I41) Servers
Version: 2.40_10-26-2020 **(Recommended)**
Filename: I41_2.40_10_26_2020.fwpkg

**Important Note!**

**Important Notes:**

This version of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2020.2 guidance.

**Deliverable Name:**

HPE ProLiant BL460c Gen10 System ROM - I41

**Release Version:**

2.40_10-26-2020

**Last Recommended or Critical Revision:**

2.40_10-26-2020

**Previous Revision:**

2.36_07-16-2020

**Firmware Dependencies:**

None

**Enhancements / New Features:**

Added a new BIOS/Platform Configuration (RBSU) option to Memory Options called Refresh Watermarks. When selecting the Low Watermark setting, the memory controller will help reduce susceptibility to a DDR4 RowHammer attack. It is expected that a memory performance impact will be seen when enabling the Low Watermark setting. The default operation of the system has not changed and customers wanting to provide additional RowHammer protection should enable this setting.

Added support to BIOS/Platform Configuration (RBSU) to allow importing and exporting Secure Boot signature lists as a signed binary file. This is useful to import the Microsoft revocation list binary file into the Secure Boot DBX as found on the UEFI forum at https://uefi.org/revocationlistfile.

Updated the System ROM to allow for an increased amount of 64-bit Memory Mapped I/O available for third party options cards.

Updated the System ROM support for One Button Secure Erase functionality with the latest HPE option devices.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

**Problems Fixed:**

This version of the system ROM includes updates to the Intel Memory Reference Code which may help improve memory stability for systems configured with two DIMMs per channel. Please consult Intel sighting documentation for more details on the improvements included in the Intel IPU.2.2020 release. This issue is not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigations for security vulnerabilities documented as CVE-2020-8696. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-0381. The Intel microcode patches included in this release are version 0x02006A08 (CPUID 50654), 0x04003003 (CPUID 50656) and 0x05003003 (CPUID 50567). These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS advisories and security vulnerabilities documented as CVE-2020-0587, CVE-2020-0588, CVE-2020-0590, CVE-2020-0591, CVE-2020-0592 and CVE-2020-0593. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00358. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS platform code advisories and security vulnerabilities documented as CVE-2020-8738, CVE-2020-8739, CVE-2020-8740, and CVE-2020-8764. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00390. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which addressed an issue where the system may get stuck in a reboot loop during memory training. This issue was introduced with the v2.30 System ROM. This issue was not unique to HPE servers.

Addressed an issue where the memory locality of the ACPI SLIT table was not being created properly. In rare cases, the incorrect ACPI SLIT values could cause unexpected impacts to system performance. This issue was introduced in the v2.10 version of the System ROM and was not seen with previous versions of the System ROM.

Addressed an issue where NVMe Hot-plug and Hot-add would not function properly with VMware. This issue did not impact NVMe Hot-plug or Hot-add with other operating systems.

Addressed an issue where the system would not properly call out a memory replacement event in the Integrated Management Log (IML) if an uncorrected memory failure occurred during an Advanced Double DRAM Device Correction (ADDDC) sparing operation. This fix only impacts the incorrect logging of these events and does not impact the normal operation of the system in terms of causing uncorrected memory failures or causing any change to the operation of A3DC functionality. This issue only impacts systems configured for fast Fault Tolerant Memory Mode (ADDDC).

Addressed an issue where the BIOS/Platform Configuration (RBSU) option for the Extended Memory Test could be automatically disabled after a system reboot. This issue was introduced with the v2.30 System ROM and was not seen with earlier version of the System ROM.

**Known Issues:**

None

**Fixes**

**Important Notes:**

This version of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2020.2 guidance.

**Firmware Dependencies:**

None

**Problems Fixed:**

This version of the system ROM includes updates to the Intel Memory Reference Code which may help improve memory stability for systems configured with two DIMMs per channel. Please consult Intel sighting documentation for more details on the improvements included in the Intel IPU.2.2020 release. This issue is not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigations for security vulnerabilities documented as CVE-2020-8696. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-0381. The Intel microcode patches included in this release are version 0x02006A08 (CPUID 50654), 0x04003003 (CPUID 50656) and 0x05003003 (CPUID 50567). These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS advisories and security vulnerabilities documented as CVE-2020-0587, CVE-2020-0588, CVE-2020-0590, CVE-2020-0591, CVE-2020-0592 and CVE-2020-0593. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00358. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS platform code advisories and security vulnerabilities documented as CVE-2020-8738, CVE-2020-8739, CVE-2020-8740, and CVE-2020-8764. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00390. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which addressed an issue where the system may get stuck in a reboot loop during memory training. This issue was introduced with the v2.30 System ROM. This issue was not unique to HPE servers.

Addressed an issue where the memory locality of the ACPI SLIT table was not being created properly. In rare cases, the incorrect ACPI SLIT values could cause unexpected impacts to system performance. This issue was introduced in the v2.10 version of the System ROM and was not seen with previous versions of the System ROM.

Addressed an issue where NVMe Hot-plug and Hot-add would not function properly with VMware. This issue did not impact NVMe Hot-plug or Hot-add with other operating systems.

Addressed an issue where the system would not properly call out a memory replacement event in the Integrated Management Log (IML) if an uncorrected memory failure occurred during an Advanced Double DRAM Device Correction (ADDDC) sparing operation. This fix only impacts the incorrect logging of these events and does not impact the normal operation of the system in terms of causing uncorrected memory failures or causing any change to the operation of A3DC functionality. This issue only impacts systems configured for fast Fault Tolerant Memory Mode (ADDDC).

Addressed an issue where the BIOS/Platform Configuration (RBSU) option for the Extended Memory Test could be automatically disabled after a system reboot. This issue was introduced with the v2.30 System ROM and was not seen with earlier version of the System ROM.

**Known Issues:**

None

**Enhancements**

Added a new BIOS/Platform Configuration (RBSU) option to Memory Options called Refresh Watermarks. When selecting the Low Watermark setting, the memory controller will help reduce susceptibility to a DDR4 RowHammer attack. It is expected that a memory performance impact will be seen when enabling the Low Watermark setting. The default operation of the system has not changed and customers wanting to provide additional RowHammer protection should enable this setting.

Added support to BIOS/Platform Configuration (RBSU) to allow importing and exporting Secure Boot signature lists as a signed binary file. This is useful to import the Microsoft revocation list binary file into the Secure Boot DBX as found on the UEFI forum at https://uefi.org/revocationlistfile.

Updated the System ROM to allow for an increased amount of 64-bit Memory Mapped I/O available for third party options cards.

Updated the System ROM support for One Button Secure Erase functionality with the latest HPE option devices.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

---

ROM Flash Firmware Package - HPE ProLiant DL160 Gen10/DL180 Gen10 (U31) Servers
Version: 2.40_10-26-2020 **(Recommended)**
Filename: U31_2.40_10_26_2020.fwpkg

**Important Note!**

**Important Notes:**

This version of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2020.2 guidance.

**Deliverable Name:**

HPE ProLiant DL160 Gen10/DL180 Gen10 System ROM - U31

**Release Version:**

2.40_10-26-2020

**Last Recommended or Critical Revision:**

2.40_10-26-2020

**Previous Revision:**

2.36_07-16-2020

**Firmware Dependencies:**

None

**Enhancements/New Features:**

Added a new BIOS/Platform Configuration (RBSU) option to Memory Options called Refresh Watermarks. When selecting the Low Watermark setting, the memory controller will help reduce susceptibility to a DDR4 RowHammer attack. It is expected that a memory performance impact will be seen when enabling the Low Watermark setting. The default operation of the system has not changed and customers wanting to provide additional RowHammer protection should enable this setting.

Added support to BIOS/Platform Configuration (RBSU) to allow importing and exporting Secure Boot signature lists as a signed binary file. This is useful to import the Microsoft revocation list binary file into the Secure Boot DBX as found on the UEFI forum at https://uefi.org/revocationlistfile.

Updated the System ROM to allow for an increased amount of 64-bit Memory Mapped I/O available for third party options cards.

Updated the System ROM support for One Button Secure Erase functionality with the latest HPE option devices.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

**Problems Fixed:**

This version of the system ROM includes updates to the Intel Memory Reference Code which may help improve memory stability for systems configured with two DIMMs per channel. Please consult Intel sighting documentation for more details on the improvements included in the Intel IPU.2.2020 release. This issue is not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigations for security vulnerabilities documented as CVE-2020-8696. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-0381. The Intel microcode patches included in this release are version 0x02006A08 (CPUID 50654), 0x04003003 (CPUID 50656) and 0x05003003 (CPUID 50567). These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS advisories and security vulnerabilities documented as CVE-2020-0587, CVE-2020-0588, CVE-2020-0590, CVE-2020-0591, CVE-2020-0592 and CVE-2020-0593. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00358. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS platform code advisories and security vulnerabilities documented as CVE-2020-8738, CVE-2020-8739, CVE-2020-8740, and CVE-2020-8764. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00390. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which addressed an issue where the system may get stuck in a reboot loop during memory training. This issue was introduced with the v2.30 System ROM. This issue was not unique to HPE servers

Addressed an issue where the memory locality of the ACPI SLIT table was not being created properly. In rare cases, the incorrect ACPI SLIT values could cause unexpected impacts to system performance. This issue was introduced in the v2.10 version of the System ROM and was not seen with previous versions of the System ROM.

Addressed an issue where NVMe Hot-plug and Hot-add would not function properly with VMware. This issue did not impact NVMe Hot-plug or Hot-add with other operating systems.

Addressed an issue where the system would not properly call out a memory replacement event in the Integrated Management Log (IML) if an uncorrected memory failure occurred during an Advanced Double DRAM Device Correction (ADDDC) sparing operation. This fix only impacts the incorrect logging of these events and does not impact the normal operation of the system in terms of causing uncorrected memory failures or causing any change to the operation of A3DC functionality. This issue only impacts systems configured for fast Fault Tolerant Memory Mode (ADDDC).

Addressed an issue where the BIOS/Platform Configuration (RBSU) option for the Extended Memory Test could be automatically disabled after a system reboot. This issue was introduced with the v2.30 System ROM and was not seen with earlier version of the System ROM.

**Known Issues:**

None

**Fixes**

**Important Notes:**

This version of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2020.2 guidance.

**Firmware Dependencies:**

None

**Problems Fixed:**

This version of the system ROM includes updates to the Intel Memory Reference Code which may help improve memory stability for systems configured with two DIMMs per channel. Please consult Intel sighting documentation for more details on the improvements included in the Intel IPU.2.2020 release. This issue is not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigations for security vulnerabilities documented as CVE-2020-8696. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-0381. The Intel microcode patches included in this release are version 0x02006A08 (CPUID 50654), 0x04003003 (CPUID 50656) and 0x05003003 (CPUID 50567). These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS advisories and security vulnerabilities documented as CVE-2020-0587, CVE-2020-0588, CVE-2020-0590, CVE-2020-0591, CVE-2020-0592 and CVE-2020-0593. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00358. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS platform code advisories and security vulnerabilities documented as CVE-2020-8738, CVE-2020-8739, CVE-2020-8740, and CVE-2020-8764. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00390. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which addressed an issue where the system may get stuck in a reboot loop during memory training. This issue was introduced with the v2.30 System ROM. This issue was not unique to HPE servers

Addressed an issue where the memory locality of the ACPI SLIT table was not being created properly. In rare cases, the incorrect ACPI SLIT values could cause unexpected impacts to system performance. This issue was introduced in the v2.10 version of the System ROM and was not seen with previous versions of the System ROM.

Addressed an issue where NVMe Hot-plug and Hot-add would not function properly with VMware. This issue did not impact NVMe Hot-plug or Hot-add with other operating systems.

Addressed an issue where the system would not properly call out a memory replacement event in the Integrated Management Log (IML) if an uncorrected memory failure occurred during an Advanced Double DRAM Device Correction (ADDDC) sparing operation. This fix only impacts the incorrect logging of these events and does not impact the normal operation of the system in terms of causing uncorrected memory failures or causing any change to the operation of A3DC functionality. This issue only impacts systems configured for fast Fault Tolerant Memory Mode (ADDDC).

Addressed an issue where the BIOS/Platform Configuration (RBSU) option for the Extended Memory Test could be automatically disabled after a system reboot. This issue was introduced with the v2.30 System ROM and was not seen with earlier version of the System ROM.

**Known Issues:**

None

**Enhancements**

Added a new BIOS/Platform Configuration (RBSU) option to Memory Options called Refresh Watermarks. When selecting the Low Watermark setting, the memory controller will help reduce susceptibility to a DDR4 RowHammer attack. It is expected that a memory performance impact will be seen when enabling the Low Watermark setting. The default operation of the system has not changed and customers wanting to provide additional RowHammer protection should enable this setting.

Added support to BIOS/Platform Configuration (RBSU) to allow importing and exporting Secure Boot signature lists as a signed binary file. This is useful to import the Microsoft revocation list binary file into the Secure Boot DBX as found on the UEFI forum at https://uefi.org/revocationlistfile.

Updated the System ROM to allow for an increased amount of 64-bit Memory Mapped I/O available for third party options cards.

Updated the System ROM support for One Button Secure Erase functionality with the latest HPE option devices.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

---

ROM Flash Firmware Package - HPE ProLiant DL20 Gen10 (U43) Servers
Version: 2.20_10-27-2020 **(Recommended)**
Filename: U43_2.20_10_27_2020.fwpkg

**Important Note!**

**Important Notes:**

This version of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2020.2 guidance.

**Deliverable Name:**

HPE ProLiant DL20 Gen10 System ROM - U43

**Release Version:**

2.20_10-27-2020

**Last Recommended or Critical Revision:**

2.20_10-27-2020

**Previous Revision:**

2.18_06-24-2020

**Firmware Dependencies:**

None

**Enhancements/New Features:**

Added a new BIOS/Platform Configuration (RBSU) option to Memory Options called Refresh Watermarks. When selecting the Low Watermark setting, the memory controller will help reduce susceptibility to a DDR4 RowHammer attack. It is expected that a memory performance impact will be seen when enabling the Low Watermark setting. The default operation of the system has not changed and customers wanting to provide additional RowHammer protection should enable this setting.

Added support to BIOS/Platform Configuration (RBSU) to allow importing and exporting Secure Boot signature lists as a signed binary file. This is useful to import the Microsoft revocation list binary file into the Secure Boot DBX as found on the UEFI forum at https://uefi.org/revocationlistfile.

Updated the System ROM support for One Button Secure Erase functionality with the latest HPE option devices.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

**Problems Fixed:**

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigations for security vulnerabilities documented as CVE-2020-8696, CVE-2020-8694 and CVE-2020-8695. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00381 and INTEL-SA-00389. The Intel microcode patches included in this release are version 0x000000DE (CPUIDs 906ED, 906EC, 906EB and 906EA). These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS advisories and security vulnerabilities documented as CVE-2020-0593. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00358. These issues are not unique to HPE servers.

Addressed an issue where the "Minimum Processor Idle Power Package C-State" RBSU option was missing.

**Known Issues:**

None

**Fixes**

**Important Notes:**

This version of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2020.2 guidance.

**Firmware Dependencies:**

None

**Problems Fixed:**

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigations for security vulnerabilities documented as CVE-2020-8696, CVE-2020-8694 and CVE-2020-8695. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00381 and INTEL-SA-00389. The Intel microcode patches included in this release are version 0x000000DE (CPUIDs 906ED, 906EC, 906EB and 906EA). These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS advisories and security vulnerabilities documented as CVE-2020-0593. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00358. These issues are not unique to HPE servers.

Addressed an issue where the "Minimum Processor Idle Power Package C-State" RBSU option was missing.

**Known Issues:**

None

**Enhancements**

Added a new BIOS/Platform Configuration (RBSU) option to Memory Options called Refresh Watermarks. When selecting the Low Watermark setting, the memory controller will help reduce susceptibility to a DDR4 RowHammer attack. It is expected that a memory performance impact will be seen when enabling the Low Watermark setting. The default

operation of the system has not changed and customers wanting to provide additional RowHammer protection should enable this setting.

Added support to BIOS/Platform Configuration (RBSU) to allow importing and exporting Secure Boot signature lists as a signed binary file. This is useful to import the Microsoft revocation list binary file into the Secure Boot DBX as found on the UEFI forum at https://uefi.org/revocationlistfile.

Updated the System ROM support for One Button Secure Erase functionality with the latest HPE option devices.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

---

ROM Flash Firmware Package - HPE ProLiant DL325 Gen10 (A41) Servers
Version: 2.42_07-17-2020 **(Recommended)**
Filename: A41_2.42_07_17_2020.fwpkg

**Important Note!**

**Important Notes:**

None

**Deliverable Name:**

HPE ProLiant DL325 Gen10 System ROM - A41

**Release Version:**

2.42_07-17-2020

**Last Recommended or Critical Revision:**

2.42_07-17-2020

**Previous Revision:**

2.40_05-11-2020

**Firmware Dependencies:**

None

**Enhancements/New Features:**

Added a new BIOS/Platform Configuration (RBSU) option for DRAM Burst Refresh Mode to provide mitigation for TRRespass and Targeted Row Refresh exploits. This option should be configured to Disabled to mitigate the TRRespass vulnerability. Setting this option to Disabled may have a minimal impact to system performance. The default setting is Enabled.

Added a new BIOS/Platform Configuration (RBSU) option in the Minimum Processor Idle Power Core C-State setting for C1 State. This option allows for power savings during certain workloads without the performance impacts of C6 State.

**Problems Fixed:**

Addressed an issue where uncorrectable memory errors are seen when running memory intensive workloads with LRDIMMs.

Address an issue that could cause a slight degradation of performance.

Resolved an issue with NVMe hot add or removal which may result in an unrecoverable I/O error reported in the Integrated Management Log (IML).

Addressed an issue where the UEFI Shell command GetPciRom may not display information for PCI expansion device drivers.

Addressed an extremely intermittent issue with AMD Epyc 1st Gen processors that would cause a critical error and system reset.

**Known Issues:**

None

**Fixes**

**Important Notes:**

None

**Firmware Dependencies:**

None

**Problems Fixed:**

Addressed an issue where uncorrectable memory errors are seen when running memory intensive workloads with LRDIMMs.

Address an issue that could cause a slight degradation of performance.

Resolved an issue with NVMe hot add or removal which may result in an unrecoverable I/O error reported in the Integrated Management Log (IML).

Addressed an issue where the UEFI Shell command GetPciRom may not display information for PCI expansion device drivers.

Addressed an extremely intermittent issue with AMD Epyc 1st Gen processors that would cause a critical error and system reset.

**Known Issues:**

None

**Enhancements**

Added a new BIOS/Platform Configuration (RBSU) option for DRAM Burst Refresh Mode to provide mitigation for TRRespass and Targeted Row Refresh exploits. This option should be configured to Disabled to mitigate the TRRespass vulnerability. Setting this option to Disabled may have a minimal impact to system performance. The default setting is Enabled.

Added a new BIOS/Platform Configuration (RBSU) option in the Minimum Processor Idle Power Core C-State setting for C1 State. This option allows for power savings during certain workloads without the performance impacts of C6 State.

---

ROM Flash Firmware Package - HPE ProLiant DL360 Gen10 (U32) Servers
Version: 2.40_10-26-2020 **(Recommended)**
Filename: U32_2.40_10_26_2020.fwpkg

## Important Note!

**Important Notes:**

This version of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2020.2 guidance.

**Deliverable Name:**

HPE ProLiant DL360 Gen10 System ROM - U32

**Release Version:**

2.40_10-26-2020

**Last Recommended or Critical Revision:**

2.40_10-26-2020

**Previous Revision:**

2.36_07-16-2020

**Firmware Dependencies:**

None

**Enhancements/New Features:**

Added a new BIOS/Platform Configuration (RBSU) option to Memory Options called Refresh Watermarks. When selecting the Low Watermark setting, the memory controller will help reduce susceptibility to a DDR4 RowHammer attack. It is expected that a memory performance impact will be seen when enabling the Low Watermark setting. The default operation of the system has not changed and customers wanting to provide additional RowHammer protection should enable this setting.

Added support to BIOS/Platform Configuration (RBSU) to allow importing and exporting Secure Boot signature lists as a signed binary file. This is useful to import the Microsoft revocation list binary file into the Secure Boot DBX as found on the UEFI forum at https://uefi.org/revocationlistfile.

Updated the System ROM to allow for an increased amount of 64-bit Memory Mapped I/O available for third party options cards.

Updated the System ROM support for One Button Secure Erase functionality with the latest HPE option devices.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

**Problems Fixed:**

This version of the system ROM includes updates to the Intel Memory Reference Code which may help improve memory stability for systems configured with two DIMMs per channel. Please consult Intel sighting documentation for more details on the improvements included in the Intel IPU.2.2020 release. This issue is not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigations for security vulnerabilities documented as CVE-2020-8696. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-0381. The Intel microcode patches included in this release are version 0x02006A08 (CPUID 50654), 0x04003003 (CPUID 50656) and 0x05003003 (CPUID 50567). These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS advisories and security vulnerabilities documented as CVE-2020-0587, CVE-2020-0588, CVE-2020-0590, CVE-2020-0591, CVE-2020-0592 and CVE-2020-0593. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00358. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS platform code advisories and security vulnerabilities documented as CVE-2020-8738, CVE-2020-8739, CVE-2020-8740, and CVE-2020-8764. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00390. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which addressed an issue where the system may get stuck in a reboot loop during memory training. This issue was introduced with the v2.30 System ROM. This issue was not unique to HPE servers

Addressed an issue where the memory locality of the ACPI SLIT table was not being created properly. In rare cases, the incorrect ACPI SLIT values could cause unexpected impacts to system performance. This issue was introduced in the v2.10 version of the System ROM and was not seen with previous versions of the System ROM.

Addressed an issue where NVMe Hot-plug and Hot-add would not function properly with VMware. This issue did not impact NVMe Hot-plug or Hot-add with other operating systems.

Addressed an issue where the system would not properly call out a memory replacement event in the Integrated Management Log (IML) if an uncorrected memory failure occurred during an Advanced Double DRAM Device Correction (ADDDC) sparing operation. This fix only impacts the incorrect logging of these events and does not impact the normal operation of the system in terms of causing uncorrected memory failures or causing any change to the operation of A3DC functionality. This issue only impacts systems configured for fast Fault Tolerant Memory Mode (ADDDC).

Addressed an issue where the BIOS/Platform Configuration (RBSU) option for the Extended Memory Test could be automatically disabled after a system reboot. This issue was introduced with the v2.30 System ROM and was not seen with earlier version of the System ROM.

**Known Issues:**

None

## Fixes

**Important Notes:**

This version of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2020.2 guidance.

**Firmware Dependencies:**

None

**Problems Fixed:**

This version of the system ROM includes updates to the Intel Memory Reference Code which may help improve memory stability for systems configured with two DIMMs per channel. Please consult Intel sighting documentation for more details on the improvements included in the Intel IPU.2.2020 release. This issue is not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigations for security vulnerabilities documented as CVE-2020-8696. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-0381. The Intel microcode patches included in this release are version 0x02006A08 (CPUID 50654), 0x04003003 (CPUID 50656) and 0x05003003 (CPUID 50567). These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS advisories and security vulnerabilities documented as CVE-2020-0587, CVE-2020-0588, CVE-2020-0590, CVE-2020-0591, CVE-2020-0592 and CVE-2020-0593. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00358. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS platform code advisories and security vulnerabilities documented as CVE-2020-8738, CVE-2020-8739, CVE-2020-8740, and CVE-2020-8764. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00390. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which addressed an issue where the system may get stuck in a reboot loop during memory

training. This issue was introduced with the v2.30 System ROM. This issue was not unique to HPE servers

Addressed an issue where the memory locality of the ACPI SLIT table was not being created properly. In rare cases, the incorrect ACPI SLIT values could cause unexpected impacts to system performance. This issue was introduced in the v2.10 version of the System ROM and was not seen with previous versions of the System ROM.

Addressed an issue where NVMe Hot-plug and Hot-add would not function properly with VMware. This issue did not impact NVMe Hot-plug or Hot-add with other operating systems.

Addressed an issue where the system would not properly call out a memory replacement event in the Integrated Management Log (IML) if an uncorrected memory failure occurred during an Advanced Double DRAM Device Correction (ADDDC) sparing operation. This fix only impacts the incorrect logging of these events and does not impact the normal operation of the system in terms of causing uncorrected memory failures or causing any change to the operation of A3DC functionality. This issue only impacts systems configured for fast Fault Tolerant Memory Mode (ADDDC).

Addressed an issue where the BIOS/Platform Configuration (RBSU) option for the Extended Memory Test could be automatically disabled after a system reboot. This issue was introduced with the v2.30 System ROM and was not seen with earlier version of the System ROM.

**Known Issues:**

None

**Enhancements**

Added a new BIOS/Platform Configuration (RBSU) option to Memory Options called Refresh Watermarks. When selecting the Low Watermark setting, the memory controller will help reduce susceptibility to a DDR4 RowHammer attack. It is expected that a memory performance impact will be seen when enabling the Low Watermark setting. The default operation of the system has not changed and customers wanting to provide additional RowHammer protection should enable this setting.

Added support to BIOS/Platform Configuration (RBSU) to allow importing and exporting Secure Boot signature lists as a signed binary file. This is useful to import the Microsoft revocation list binary file into the Secure Boot DBX as found on the UEFI forum at https://uefi.org/revocationlistfile.

Updated the System ROM to allow for an increased amount of 64-bit Memory Mapped I/O available for third party options cards.

Updated the System ROM support for One Button Secure Erase functionality with the latest HPE option devices.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

---

ROM Flash Firmware Package - HPE ProLiant DL380 Gen10 (U30) Servers
Version: 2.40_10-26-2020 **(Recommended)**
Filename: U30_2.40_10_26_2020.fwpkg

**Important Note!**

**Important Notes:**

This version of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2020.2 guidance.

**Deliverable Name:**

HPE ProLiant DL380 Gen10 System ROM - U30

**Release Version:**

2.40_10-26-2020

**Last Recommended or Critical Revision:**

2.40_10-26-2020

**Previous Revision:**

2.36_07-16-2020

**Firmware Dependencies:**

None

**Enhancements/New Features:**

Added a new BIOS/Platform Configuration (RBSU) option to Memory Options called Refresh Watermarks. When selecting the Low Watermark setting, the memory controller will help reduce susceptibility to a DDR4 RowHammer attack. It is expected that a memory performance impact will be seen when enabling the Low Watermark setting. The default operation of the system has not changed and customers wanting to provide additional RowHammer protection should enable this setting.

Added support to BIOS/Platform Configuration (RBSU) to allow importing and exporting Secure Boot signature lists as a signed binary file. This is useful to import the Microsoft revocation list binary file into the Secure Boot DBX as found on the UEFI forum at https://uefi.org/revocationlistfile.

Updated the System ROM to allow for an increased amount of 64-bit Memory Mapped I/O available for third party options cards.

Updated the System ROM support for One Button Secure Erase functionality with the latest HPE option devices.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

**Problems Fixed:**

This version of the system ROM includes updates to the Intel Memory Reference Code which may help improve memory stability for systems configured with two DIMMs per channel. Please consult Intel sighting documentation for more details on the improvements included in the Intel IPU.2.2020 release. This issue is not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigations for security vulnerabilities documented as CVE-2020-8696. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-0381. The Intel microcode patches included in this release are version 0x02006A08 (CPUID 50654), 0x04003003 (CPUID 50656) and 0x05003003 (CPUID 50567). These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS advisories and security vulnerabilities documented as CVE-2020-0587, CVE-2020-0588, CVE-2020-0590, CVE-2020-0591, CVE-2020-0592 and CVE-2020-0593. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00358. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS platform code advisories and security vulnerabilities documented as CVE-2020-8738, CVE-2020-8739, CVE-2020-8740, and CVE-2020-8764. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00390. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which addressed an issue where the system may get stuck in a reboot loop during memory training. This issue was introduced with the v2.30 System ROM. This issue was not unique to HPE servers

Addressed an issue where the memory locality of the ACPI SLIT table was not being created properly. In rare cases, the incorrect ACPI SLIT values could cause unexpected impacts to system performance. This issue was introduced in the v2.10 version of the System ROM and was not seen with previous versions of the System ROM.

Addressed an issue where NVMe Hot-plug and Hot-add would not function properly with VMware. This issue did not impact NVMe Hot-plug or Hot-add with other operating systems.

Addressed an issue where the system would not properly call out a memory replacement event in the Integrated Management Log (IML) if an uncorrected memory failure occurred during an Advanced Double DRAM Device Correction (ADDDC) sparing operation. This fix only impacts the incorrect logging of these events and does not impact the normal operation of the system in terms of causing uncorrected memory failures or causing any change to the operation of A3DC functionality. This issue only impacts systems configured for fast Fault Tolerant Memory Mode (ADDDC).

Addressed an issue where the BIOS/Platform Configuration (RBSU) option for the Extended Memory Test could be automatically disabled after a system reboot. This issue was introduced with the v2.30 System ROM and was not seen with earlier version of the System ROM.

**Known Issues:**

None

**Fixes**

**Important Notes:**

This version of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2020.2 guidance.

**Firmware Dependencies:**

None

**Problems Fixed:**

This version of the system ROM includes updates to the Intel Memory Reference Code which may help improve memory stability for systems configured with two DIMMs per channel. Please consult Intel sighting documentation for more details on the improvements included in the Intel IPU.2.2020 release. This issue is not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigations for security vulnerabilities documented as CVE-2020-8696. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-0381. The Intel microcode patches included in this release are version 0x02006A08 (CPUID 50654), 0x04003003 (CPUID 50656) and 0x05003003 (CPUID 50567). These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS advisories and security vulnerabilities documented as CVE-2020-0587, CVE-2020-0588, CVE-2020-0590, CVE-2020-0591, CVE-2020-0592 and CVE-2020-0593. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00358. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS platform code advisories and security vulnerabilities documented as CVE-2020-8738, CVE-2020-8739, CVE-2020-8740, and CVE-2020-8764. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00390. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which addressed an issue where the system may get stuck in a reboot loop during memory training. This issue was introduced with the v2.30 System ROM. This issue was not unique to HPE servers

Addressed an issue where the memory locality of the ACPI SLIT table was not being created properly. In rare cases, the incorrect ACPI SLIT values could cause unexpected impacts to system performance. This issue was introduced in the v2.10 version of the System ROM and was not seen with previous versions of the System ROM.

Addressed an issue where NVMe Hot-plug and Hot-add would not function properly with VMware. This issue did not impact NVMe Hot-plug or Hot-add with other operating systems.

Addressed an issue where the system would not properly call out a memory replacement event in the Integrated Management Log (IML) if an uncorrected memory failure occurred during an Advanced Double DRAM Device Correction (ADDDC) sparing operation. This fix only impacts the incorrect logging of these events and does not impact the normal operation of the system in terms of causing uncorrected memory failures or causing any change to the operation of A3DC functionality. This issue only impacts systems configured for fast Fault Tolerant Memory Mode (ADDDC).

Addressed an issue where the BIOS/Platform Configuration (RBSU) option for the Extended Memory Test could be automatically disabled after a system reboot. This issue was introduced with the v2.30 System ROM and was not seen with earlier version of the System ROM.

**Known Issues:**

None

**Enhancements**

Added a new BIOS/Platform Configuration (RBSU) option to Memory Options called Refresh Watermarks. When selecting the Low Watermark setting, the memory controller will help reduce susceptibility to a DDR4 RowHammer attack. It is expected that a memory performance impact will be seen when enabling the Low Watermark setting. The default operation of the system has not changed and customers wanting to provide additional RowHammer protection should enable this setting.

Added support to BIOS/Platform Configuration (RBSU) to allow importing and exporting Secure Boot signature lists as a signed binary file. This is useful to import the Microsoft revocation list binary file into the Secure Boot DBX as found on the UEFI forum at https://uefi.org/revocationlistfile.

Updated the System ROM to allow for an increased amount of 64-bit Memory Mapped I/O available for third party options cards.

Updated the System ROM support for One Button Secure Erase functionality with the latest HPE option devices.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

---

ROM Flash Firmware Package - HPE ProLiant DL385 Gen10 (A40) Servers
Version: 2.42_07-17-2020 **(Recommended)**
Filename: A40_2.42_07_17_2020.fwpkg

**Important Note!**

**Important Notes:**

None

**Deliverable Name:**

HPE ProLiant DL385 Gen10 System ROM - A40

**Release Version:**

2.42_07-17-2020

**Last Recommended or Critical Revision:**

2.42_07-17-2020

**Previous Revision:**

2.40_05-11-2020

**Firmware Dependencies:**

None

**Enhancements/New Features:**

Added a new BIOS/Platform Configuration (RBSU) option for DRAM Burst Refresh Mode to provide mitigation for TRRespass and Targeted Row Refresh exploits. This option should be configured to Disabled to mitigate the TRRespass vulnerability. Setting this option to Disabled may have a minimal impact to system performance. The default setting is Enabled.

Added a new BIOS/Platform Configuration (RBSU) option in the Minimum Processor Idle Power Core C-State setting for C1 State. This option allows for power savings during certain workloads without the performance impacts of C6 State.

**Problems Fixed:**

Addressed an issue where uncorrectable memory errors are seen when running memory intensive workloads with LRDIMMs.

Address an issue that could cause a slight degradation of performance.

Resolved an issue with NVMe hot add or removal which may result in an unrecoverable I/O error reported in the Integrated Management Log (IML).

Addressed issue where the UEFI Shell command GetPciRom may not display information for PCI expansion device drivers.

Addressed an extremely intermittent issue with AMD Epyc 1st Gen processors that would cause a critical error and system reset.

**Known Issues:**

None

**Fixes**

**Important Notes:**

None

**Firmware Dependencies:**

None

**Problems Fixed:**

Addressed an issue where uncorrectable memory errors are seen when running memory intensive workloads with LRDIMMs.

Address an issue that could cause a slight degradation of performance.

Resolved an issue with NVMe hot add or removal which may result in an unrecoverable I/O error reported in the Integrated Management Log (IML).

Addressed an issue where the UEFI Shell command GetPciRom may not display information for PCI expansion device drivers.

Addressed an extremely intermittent issue with AMD Epyc 1st Gen processors that would cause a critical error and system reset.

**Known Issues:**

None

**Enhancements**

Added a new BIOS/Platform Configuration (RBSU) option for DRAM Burst Refresh Mode to provide mitigation for TRRespass and Targeted Row Refresh exploits. This option should be configured to Disabled to mitigate the TRRespass vulnerability. Setting this option to Disabled may have a minimal impact to system performance. The default setting is Enabled.

Added a new BIOS/Platform Configuration (RBSU) option in the Minimum Processor Idle Power Core C-State setting for C1 State. This option allows for power savings during certain workloads without the performance impacts of C6 State.

---

ROM Flash Firmware Package - HPE ProLiant DL560 Gen10/DL580 Gen10 (U34) Servers
Version: 2.40_10-26-2020 **(Recommended)**
Filename: U34_2.40_10_26_2020.fwpkg

**Important Note!**

**Important Notes:**

This version of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2020.2 guidance.

**Deliverable Name:**

HPE ProLiant DL560 Gen10/DL580 Gen10 System ROM - U34

**Release Version:**

2.40_10-26-2020

**Last Recommended or Critical Revision:**

2.40_10-26-2020

**Previous Revision:**

2.36_07-16-2020

**Firmware Dependencies:**

None

**Enhancements/New Features:**

Added a new BIOS/Platform Configuration (RBSU) option to Memory Options called Refresh Watermarks. When selecting the Low Watermark setting, the memory controller will help reduce susceptibility to a DDR4 RowHammer attack. It is expected that a memory performance impact will be seen when enabling the Low Watermark setting. The default operation of the system has not changed and customers wanting to provide additional RowHammer protection should enable this setting.

Added support to BIOS/Platform Configuration (RBSU) to allow importing and exporting Secure Boot signature lists as a signed binary file. This is useful to import the Microsoft revocation list binary file into the Secure Boot DBX as found on the UEFI forum at https://uefi.org/revocationlistfile.

Updated the System ROM to allow for an increased amount of 64-bit Memory Mapped I/O available for third party options cards.

Updated the System ROM support for One Button Secure Erase functionality with the latest HPE option devices.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

**Problems Fixed:**

This version of the system ROM includes updates to the Intel Memory Reference Code which may help improve memory stability for systems configured with two DIMMs per channel. Please consult Intel sighting documentation for more details on the improvements included in the Intel IPU.2.2020 release. This issue is not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigations for security vulnerabilities documented as CVE-2020-8696. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-0381. The Intel microcode patches included in this release are version 0x02006A08 (CPUID 50654), 0x04003003 (CPUID 50656) and 0x05003003 (CPUID 50567). These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS advisories and security vulnerabilities documented as CVE-2020-0587, CVE-2020-0588, CVE-2020-0590, CVE-2020-0591, CVE-2020-0592 and CVE-2020-0593. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00358. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS platform code advisories and security vulnerabilities documented as CVE-2020-8738, CVE-2020-8739, CVE-2020-8740, and CVE-2020-8764. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00390. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which addressed an issue where the system may get stuck in a reboot loop during memory training. This issue was introduced with the v2.30 System ROM. This issue was not unique to HPE servers

Addressed an issue where the memory locality of the ACPI SLIT table was not being created properly. In rare cases, the incorrect ACPI SLIT values could cause unexpected impacts to system performance. This issue was introduced in the v2.10 version of the System ROM and was not seen with previous versions of the System ROM.

Addressed an issue where NVMe Hot-plug and Hot-add would not function properly with VMware. This issue did not impact NVMe Hot-plug or Hot-add with other operating systems.

Addressed an issue where the system would not properly call out a memory replacement event in the Integrated Management Log (IML) if an uncorrected memory failure occurred during an Advanced Double DRAM Device Correction (ADDDC) sparing operation. This fix only impacts the incorrect logging of these events and does not impact the normal operation of the system in terms of causing uncorrected memory failures or causing any change to the operation of A3DC functionality. This issue only impacts systems configured for fast Fault Tolerant Memory Mode (ADDDC).

Addressed an issue where the BIOS/Platform Configuration (RBSU) option for the Extended Memory Test could be automatically disabled after a system reboot. This issue was introduced with the v2.30 System ROM and was not seen with earlier version of the System ROM.

Addressed an issue where the device in Slot 3 could not be detected when Slot 2 was empty.

**Known Issues:**

None

## Fixes

**Important Notes:**

This version of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2020.2 guidance.

**Firmware Dependencies:**

None

**Problems Fixed:**

This version of the system ROM includes updates to the Intel Memory Reference Code which may help improve memory stability for systems configured with two DIMMs per channel. Please consult Intel sighting documentation for more details on the improvements included in the Intel IPU.2.2020 release. This issue is not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigations for security vulnerabilities documented as CVE-2020-8696. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-0381. The Intel microcode patches included in this release are version 0x02006A08 (CPUID 50654), 0x04003003 (CPUID 50656) and 0x05003003 (CPUID 50567). These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS advisories and security vulnerabilities documented as CVE-2020-0587, CVE-2020-0588, CVE-2020-0590, CVE-2020-0591, CVE-2020-0592 and CVE-2020-0593. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00358. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS platform code advisories and security vulnerabilities documented as CVE-2020-8738, CVE-2020-8739, CVE-2020-8740, and CVE-2020-8764. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00390. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which addressed an issue where the system may get stuck in a reboot loop during memory training. This issue was introduced with the v2.30 System ROM. This issue was not unique to HPE servers

Addressed an issue where the memory locality of the ACPI SLIT table was not being created properly. In rare cases, the incorrect ACPI SLIT values could cause unexpected impacts to system performance. This issue was introduced in the v2.10 version of the System ROM and was not seen with previous versions of the System ROM.

Addressed an issue where NVMe Hot-plug and Hot-add would not function properly with VMware. This issue did not impact NVMe Hot-plug or Hot-add with other operating systems.

Addressed an issue where the system would not properly call out a memory replacement event in the Integrated Management Log (IML) if an uncorrected memory failure occurred during an Advanced Double DRAM Device Correction (ADDDC) sparing operation. This fix only impacts the incorrect logging of these events and does not impact the normal operation of the system in terms of causing uncorrected memory failures or causing any change to the operation of A3DC functionality. This issue only impacts systems configured for fast Fault Tolerant Memory Mode (ADDDC).

Addressed an issue where the BIOS/Platform Configuration (RBSU) option for the Extended Memory Test could be automatically disabled after a system reboot. This issue was introduced with the v2.30 System ROM and was not seen with earlier version of the System ROM.

Addressed an issue where the device in Slot 3 could not be detected when Slot 2 was empty.

**Known Issues:**

None

## Enhancements

Added a new BIOS/Platform Configuration (RBSU) option to Memory Options called Refresh Watermarks. When selecting the Low Watermark setting, the memory controller will help reduce susceptibility to a DDR4 RowHammer attack. It is expected that a memory performance impact will be seen when enabling the Low Watermark setting. The default operation of the system has not changed and customers wanting to provide additional RowHammer protection should enable this setting.

Added support to BIOS/Platform Configuration (RBSU) to allow importing and exporting Secure Boot signature lists as a signed binary file. This is useful to import the Microsoft revocation list binary file into the Secure Boot DBX as found on the UEFI forum at https://uefi.org/revocationlistfile.

Updated the System ROM to allow for an increased amount of 64-bit Memory Mapped I/O available for third party options cards.

Updated the System ROM support for One Button Secure Erase functionality with the latest HPE option devices.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

---

ROM Flash Firmware Package - HPE ProLiant MicroServer Gen10 Plus (U48) Servers
Version: 2.20_10-27-2020 **(Recommended)**
Filename: U48_2.20_10_27_2020.fwpkg

**Important Note!**

**Important Notes:**

None

**Deliverable Name:**

HPE ProLiant MicroServer Gen10 Plus System ROM - U48

**Release Version:**

2.20_10-27-2020

**Last Recommended or Critical Revision:**

2.20_10-27-2020

**Previous Revision:**

2.18_06-24-2020

**Firmware Dependencies:**

None

**Enhancements/New Features:**

Added a new BIOS/Platform Configuration (RBSU) option to Memory Options called Refresh Watermarks. When selecting the Low Watermark setting, the memory controller will help reduce susceptibility to a DDR4 RowHammer attack. It is expected that a memory performance impact will be seen when enabling the Low Watermark setting. The default operation of the system has not changed and customers wanting to provide additional RowHammer protection should enable this setting.

Added support to BIOS/Platform Configuration (RBSU) to allow importing and exporting Secure Boot signature lists as a signed binary file. This is useful to import the Microsoft revocation list binary file into the Secure Boot DBX as found on the UEFI forum at https://uefi.org/revocationlistfile.

Updated the System ROM support for One Button Secure Erase functionality with the latest HPE option devices.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

**Problems Fixed:**

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigations for security vulnerabilities documented as CVE-2020-8696, CVE-2020-8694 and CVE-2020-8695. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00381 and INTEL-SA-00389. The Intel microcode patches included in this release are version 0x000000DE (CPUIDs 906ED, 906EC, 906EB and 906EA). These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS advisories and security vulnerabilities documented as CVE-2020-0593. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00358. These issues are not unique to HPE servers.

**Known Issues:**

None

**Fixes**

**Important Notes:**

This version of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2020.2 guidance.

**Firmware Dependencies:**

None

**Problems Fixed:**

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigations for security vulnerabilities documented as CVE-2020-8696, CVE-2020-8694 and CVE-2020-8695. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00381 and INTEL-SA-00389. The Intel microcode patches included in this release are version 0x000000DE (CPUIDs 906ED, 906EC, 906EB and 906EA). These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS advisories and security vulnerabilities documented as CVE-2020-0593. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00358. These issues are not unique to HPE servers.

**Known Issues:**

None

**Enhancements**

Added a new BIOS/Platform Configuration (RBSU) option to Memory Options called Refresh Watermarks. When selecting the Low Watermark setting, the memory controller will help reduce susceptibility to a DDR4 RowHammer attack. It is expected that a memory performance impact will be seen when enabling the Low Watermark setting. The default operation of the system has not changed and customers wanting to provide additional RowHammer protection should enable this setting.

Added support to BIOS/Platform Configuration (RBSU) to allow importing and exporting Secure Boot signature lists as a signed binary file. This is useful to import the Microsoft revocation list binary file into the Secure Boot DBX as found on the UEFI forum at https://uefi.org/revocationlistfile.

Updated the System ROM support for One Button Secure Erase functionality with the latest HPE option devices.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

---

ROM Flash Firmware Package - HPE ProLiant ML110 Gen10 (U33) Servers
Version: 2.40_10-26-2020 **(Recommended)**
Filename: U33_2.40_10_26_2020.fwpkg

**Important Note!**

**Important Notes:**

This version of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2020.2 guidance.

**Deliverable Name:**

HPE ProLiant ML110 Gen10 System ROM - U33

**Release Version:**

2.40_10-26-2020

**Last Recommended or Critical Revision:**

2.40_10-26-2020

**Previous Revision:**

2.36_07-16-2020

**Firmware Dependencies:**

None

**Enhancements/New Features:**

Added a new BIOS/Platform Configuration (RBSU) option to Memory Options called Refresh Watermarks. When selecting the Low Watermark setting, the memory controller will help reduce susceptibility to a DDR4 RowHammer attack. It is expected that a memory performance impact will be seen when enabling the Low Watermark setting. The default operation of the system has not changed and customers wanting to provide additional RowHammer protection should enable this setting.

Added support to BIOS/Platform Configuration (RBSU) to allow importing and exporting Secure Boot signature lists as a signed binary file. This is useful to import the Microsoft revocation list binary file into the Secure Boot DBX as found on the UEFI forum at https://uefi.org/revocationlistfile.

Updated the System ROM to allow for an increased amount of 64-bit Memory Mapped I/O available for third party options cards.

Updated the System ROM support for One Button Secure Erase functionality with the latest HPE option devices.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

**Problems Fixed:**

This version of the system ROM includes updates to the Intel Memory Reference Code which may help improve memory stability for systems configured with two DIMMs per channel. Please consult Intel sighting documentation for more details on the improvements included in the Intel IPU.2.2020 release. This issue is not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigations for security vulnerabilities documented as CVE-2020-8696. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-0381. The Intel microcode patches included in this release are version 0x02006A08 (CPUID 50654), 0x04003003 (CPUID 50656) and 0x05003003 (CPUID 50567). These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS advisories and security vulnerabilities documented as CVE-2020-0587, CVE-2020-0588, CVE-2020-0590, CVE-2020-0591, CVE-2020-0592 and CVE-2020-0593. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00358. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS platform code advisories and security vulnerabilities documented as CVE-2020-8738, CVE-2020-8739, CVE-2020-8740, and CVE-2020-8764. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00390. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which addressed an issue where the system may get stuck in a reboot loop during memory training. This issue was introduced with the v2.30 System ROM. This issue was not unique to HPE servers

Addressed an issue where the memory locality of the ACPI SLIT table was not being created properly. In rare cases, the incorrect ACPI SLIT values could cause unexpected impacts to system performance. This issue was introduced in the v2.10 version of the System ROM and was not seen with previous versions of the System ROM.

Addressed an issue where NVMe Hot-plug and Hot-add would not function properly with VMware. This issue did not impact NVMe Hot-plug or Hot-add with other operating systems.

Addressed an issue where the system would not properly call out a memory replacement event in the Integrated Management Log (IML) if an uncorrected memory failure occurred during an Advanced Double DRAM Device Correction (ADDDC) sparing operation. This fix only impacts the incorrect logging of these events and does not impact the normal operation of the system in terms of causing uncorrected memory failures or causing any change to the operation of A3DC functionality. This issue only impacts systems configured for fast Fault Tolerant Memory Mode (ADDDC).

Addressed an issue where the BIOS/Platform Configuration (RBSU) option for the Extended Memory Test could be automatically disabled after a system reboot. This issue was introduced with the v2.30 System ROM and was not seen with earlier version of the System ROM.

**Known Issues:**

None

**Fixes**

**Important Notes:**

This version of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2020.2 guidance.

**Firmware Dependencies:**

None

**Problems Fixed:**

This version of the system ROM includes updates to the Intel Memory Reference Code which may help improve memory stability for systems configured with two DIMMs per channel. Please consult Intel sighting documentation for more details on the improvements included in the Intel IPU.2.2020 release. This issue is not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigations for security vulnerabilities documented as CVE-2020-8696. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-0381. The Intel microcode patches included in this release are version 0x02006A08 (CPUID 50654), 0x04003003 (CPUID 50656) and 0x05003003 (CPUID 50567). These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS advisories and security vulnerabilities documented as CVE-2020-0587, CVE-2020-0588, CVE-2020-0590, CVE-2020-0591, CVE-2020-0592 and CVE-2020-0593. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00358. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS platform code advisories and security vulnerabilities documented as CVE-2020-8738, CVE-2020-8739, CVE-2020-8740, and CVE-2020-8764. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00390. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which addressed an issue where the system may get stuck in a reboot loop during memory training. This issue was introduced with the v2.30 System ROM. This issue was not unique to HPE servers

Addressed an issue where the memory locality of the ACPI SLIT table was not being created properly. In rare cases, the incorrect ACPI SLIT values could cause unexpected impacts to system performance. This issue was introduced in the v2.10 version of the System ROM and was not seen with previous versions of the System ROM.

Addressed an issue where NVMe Hot-plug and Hot-add would not function properly with VMware. This issue did not impact NVMe Hot-plug or Hot-add with other operating systems.

Addressed an issue where the system would not properly call out a memory replacement event in the Integrated Management Log (IML) if an uncorrected memory failure occurred during an Advanced Double DRAM Device Correction (ADDDC) sparing operation. This fix only impacts the incorrect logging of these events and does not impact the normal operation of the system in terms of causing uncorrected memory failures or causing any change to the operation of A3DC functionality. This issue only impacts systems configured for fast Fault Tolerant Memory Mode (ADDDC).

Addressed an issue where the BIOS/Platform Configuration (RBSU) option for the Extended Memory Test could be automatically disabled after a system reboot. This issue was introduced with the v2.30 System ROM and was not seen with earlier version of the System ROM.

**Known Issues:**

None

**Enhancements**

Added a new BIOS/Platform Configuration (RBSU) option to Memory Options called Refresh Watermarks. When selecting the Low Watermark setting, the memory controller will help reduce susceptibility to a DDR4 RowHammer attack. It is expected that a memory performance impact will be seen when enabling the Low Watermark setting. The default operation of the system has not changed and customers wanting to provide additional RowHammer protection should enable this setting.

Added support to BIOS/Platform Configuration (RBSU) to allow importing and exporting Secure Boot signature lists as a signed binary file. This is useful to import the Microsoft revocation list binary file into the Secure Boot DBX as found on the UEFI forum at https://uefi.org/revocationlistfile.

Updated the System ROM to allow for an increased amount of 64-bit Memory Mapped I/O available for third party options cards.

Updated the System ROM support for One Button Secure Erase functionality with the latest HPE option devices.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

---

ROM Flash Firmware Package - HPE ProLiant ML30 Gen10 (U44) Servers
Version: 2.20_10-27-2020 **(Recommended)**
Filename: U44_2.20_10_27_2020.fwpkg

**Important Note!**

**Important Notes:**

This version of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2020.2 guidance.

**Deliverable Name:**

HPE ProLiant ML30 Gen10 System ROM - U44

**Release Version:**

2.20_10-27-2020

**Last Recommended or Critical Revision:**

2.20_10-27-2020

**Previous Revision:**

2.18_06-24-2020

**Firmware Dependencies:**

None

**Enhancements/New Features:**

Added a new BIOS/Platform Configuration (RBSU) option to Memory Options called Refresh Watermarks. When selecting the Low Watermark setting, the memory controller will help reduce susceptibility to a DDR4 RowHammer attack. It is expected that a memory performance impact will be seen when enabling the Low Watermark setting. The default operation of the system has not changed and customers wanting to provide additional RowHammer protection should enable this setting.

Added support to BIOS/Platform Configuration (RBSU) to allow importing and exporting Secure Boot signature lists as a signed binary file. This is useful to import the Microsoft revocation list binary file into the Secure Boot DBX as found on the UEFI forum at https://uefi.org/revocationlistfile.

Updated the System ROM support for One Button Secure Erase functionality with the latest HPE option devices.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

**Problems Fixed:**

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigations for security vulnerabilities documented as CVE-2020-8696, CVE-2020-8694 and CVE-2020-8695. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00381 and INTEL-SA-00389. The Intel microcode patches included in this release are version 0x000000DE (CPUIDs 906ED, 906EC, 906EB and 906EA). These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS advisories and security vulnerabilities documented as CVE-2020-0593. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00358. These issues are not unique to HPE servers.

Addressed an issue where the "Minimum Processor Idle Power Package C-State" RBSU option was missing.

**Known Issues:**

None

**Fixes**

**Important Notes:**

This version of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2020.2 guidance.

**Firmware Dependencies:**

None

**Problems Fixed:**

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigations for security vulnerabilities documented as CVE-2020-8696, CVE-2020-8694 and CVE-2020-8695. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00381 and INTEL-SA-00389. The Intel microcode patches included in this release are version 0x000000DE (CPUIDs 906ED, 906EC, 906EB and 906EA). These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS advisories and security vulnerabilities documented as CVE-2020-0593. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00358. These issues are not unique to HPE servers.

Addressed an issue where the "Minimum Processor Idle Power Package C-State" RBSU option was missing.

**Known Issues:**

None

**Enhancements**

Added a new BIOS/Platform Configuration (RBSU) option to Memory Options called Refresh Watermarks. When selecting the Low Watermark setting, the memory controller will help reduce susceptibility to a DDR4 RowHammer attack. It is expected that a memory performance impact will be seen when enabling the Low Watermark setting. The default operation of the system has not changed and customers wanting to provide additional RowHammer protection should enable this setting.

Added support to BIOS/Platform Configuration (RBSU) to allow importing and exporting Secure Boot signature lists as a signed binary file. This is useful to import the Microsoft revocation list binary file into the Secure Boot DBX as found on the UEFI forum at https://uefi.org/revocationlistfile.

Updated the System ROM support for One Button Secure Erase functionality with the latest HPE option devices.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

---

ROM Flash Firmware Package - HPE ProLiant ML350 Gen10 (U41) Servers
Version: 2.40_10-26-2020 **(Recommended)**
Filename: U41_2.40_10_26_2020.fwpkg

**Important Note!**

**Important Notes:**

This version of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2020.2 guidance.

**Deliverable Name:**

HPE ProLiant ML350 Gen10 System ROM - U41

**Release Version:**

2.40_10-26-2020

**Last Recommended or Critical Revision:**

2.40_10-26-2020

**Previous Revision:**

2.36_07-16-2020

**Firmware Dependencies:**

None

**Enhancements/New Features:**

Added a new BIOS/Platform Configuration (RBSU) option to Memory Options called Refresh Watermarks. When selecting the Low Watermark setting, the memory controller will help reduce susceptibility to a DDR4 RowHammer attack. It is expected that a memory performance impact will be seen when enabling the Low Watermark setting. The default operation of the system has not changed and customers wanting to provide additional RowHammer protection should enable this setting.

Added support to BIOS/Platform Configuration (RBSU) to allow importing and exporting Secure Boot signature lists as a signed binary file. This is useful to import the Microsoft revocation list binary file into the Secure Boot DBX as found on the UEFI forum at https://uefi.org/revocationlistfile.

Updated the System ROM to allow for an increased amount of 64-bit Memory Mapped I/O available for third party options cards.

Updated the System ROM support for One Button Secure Erase functionality with the latest HPE option devices.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

**Problems Fixed:**

This version of the system ROM includes updates to the Intel Memory Reference Code which may help improve memory stability for systems configured with two DIMMs per channel. Please consult Intel sighting documentation for more details on the improvements included in the Intel IPU.2.2020 release. This issue is not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigations for security vulnerabilities documented as CVE-2020-8696. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-0381. The Intel microcode patches included in this release are version 0x02006A08 (CPUID 50654), 0x04003003 (CPUID 50656) and 0x05003003 (CPUID 50567). These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS advisories and security vulnerabilities documented as CVE-2020-0587, CVE-2020-0588, CVE-2020-0590, CVE-2020-0591, CVE-2020-0592 and CVE-2020-0593. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00358. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS platform code advisories and security vulnerabilities documented as CVE-2020-8738, CVE-2020-8739, CVE-2020-8740, and CVE-2020-8764. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00390. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which addressed an issue where the system may get stuck in a reboot loop during memory training. This issue was introduced with the v2.30 System ROM. This issue was not unique to HPE servers

Addressed an issue where the memory locality of the ACPI SLIT table was not being created properly. In rare cases, the incorrect ACPI SLIT values could cause unexpected impacts to system performance. This issue was introduced in the v2.10 version of the System ROM and was not seen with previous versions of the System ROM.

Addressed an issue where NVMe Hot-plug and Hot-add would not function properly with VMware. This issue did not impact NVMe Hot-plug or Hot-add with other operating systems.

Addressed an issue where the system would not properly call out a memory replacement event in the Integrated Management Log (IML) if an uncorrected memory failure occurred during an Advanced Double DRAM Device Correction (ADDDC) sparing operation. This fix only impacts the incorrect logging of these events and does not impact the normal operation of the system in terms of causing uncorrected memory failures or causing any change to the operation of A3DC functionality. This issue only impacts systems configured for fast Fault Tolerant Memory Mode (ADDDC).

Addressed an issue where the BIOS/Platform Configuration (RBSU) option for the Extended Memory Test could be automatically disabled after a system reboot. This issue was introduced with the v2.30 System ROM and was not seen with earlier version of the System ROM.

**Known Issues:**

None

**Fixes**

**Important Notes:**

This version of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2020.2 guidance.

**Firmware Dependencies:**

None

**Problems Fixed:**

This version of the system ROM includes updates to the Intel Memory Reference Code which may help improve memory stability for systems configured with two DIMMs per channel. Please consult Intel sighting documentation for more details on the improvements included in the Intel IPU.2.2020 release. This issue is not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigations for security vulnerabilities documented as CVE-2020-8696. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-0381. The Intel microcode patches included in this release are version 0x02006A08 (CPUID 50654), 0x04003003 (CPUID 50656) and 0x05003003 (CPUID 50567). These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS advisories and security vulnerabilities documented as CVE-2020-0587, CVE-2020-0588, CVE-2020-0590, CVE-2020-0591, CVE-2020-0592 and CVE-2020-0593. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00358. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS platform code advisories and security vulnerabilities documented as CVE-2020-8738, CVE-2020-8739, CVE-2020-8740, and CVE-2020-8764. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00390. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which addressed an issue where the system may get stuck in a reboot loop during memory training. This issue was introduced with the v2.30 System ROM. This issue was not unique to HPE servers

Addressed an issue where the memory locality of the ACPI SLIT table was not being created properly. In rare cases, the incorrect ACPI SLIT values could cause unexpected impacts to system performance. This issue was introduced in the v2.10 version of the System ROM and was not seen with previous versions of the System ROM.

Addressed an issue where NVMe Hot-plug and Hot-add would not function properly with VMware. This issue did not impact NVMe Hot-plug or Hot-add with other operating systems.

Addressed an issue where the system would not properly call out a memory replacement event in the Integrated Management Log (IML) if an uncorrected memory failure occurred during an Advanced Double DRAM Device Correction (ADDDC) sparing operation. This fix only impacts the incorrect logging of these events and does not impact the normal operation of the system in terms of causing uncorrected memory failures or causing any change to the operation of A3DC functionality. This issue only impacts systems configured for fast Fault Tolerant Memory Mode (ADDDC).

Addressed an issue where the BIOS/Platform Configuration (RBSU) option for the Extended Memory Test could be automatically disabled after a system reboot. This issue was introduced with the v2.30 System ROM and was not seen with earlier version of the System ROM.

**Known Issues:**

None

**Enhancements**

Added a new BIOS/Platform Configuration (RBSU) option to Memory Options called Refresh Watermarks. When selecting the Low Watermark setting, the memory controller will help reduce susceptibility to a DDR4 RowHammer attack. It is expected that a memory performance impact will be seen when enabling the Low Watermark setting. The default operation of the system has not changed and customers wanting to provide additional RowHammer protection should enable this setting.

Added support to BIOS/Platform Configuration (RBSU) to allow importing and exporting Secure Boot signature lists as a signed binary file. This is useful to import the Microsoft revocation list binary file into the Secure Boot DBX as found on the UEFI forum at https://uefi.org/revocationlistfile.

Updated the System ROM to allow for an increased amount of 64-bit Memory Mapped I/O available for third party options cards.

Updated the System ROM support for One Button Secure Erase functionality with the latest HPE option devices.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

---

ROM Flash Firmware Package - HPE ProLiant XL230k Gen10 (U37) Server
Version: 2.40_10-26-2020 **(Recommended)**
Filename: U37_2.40_10_26_2020.fwpkg

**Important Note!**

**Important Notes:**

This version of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2020.2 guidance.

**Deliverable Name:**

HPE ProLiant XL230k Gen10 System ROM - U37

**Release Version:**

2.40_10-26-2020

**Last Recommended or Critical Revision:**

2.40_10-26-2020

**Previous Revision:**

2.36_07-16-2020

**Firmware Dependencies:**

None

**Enhancements/New Features:**

Added a new BIOS/Platform Configuration (RBSU) option to Memory Options called Refresh Watermarks. When selecting the Low Watermark setting, the memory controller will help reduce susceptibility to a DDR4 RowHammer attack. It is expected that a memory performance impact will be seen when enabling the Low Watermark setting. The default operation of the system has not changed and customers wanting to provide additional RowHammer protection should enable this setting.

Added support to BIOS/Platform Configuration (RBSU) to allow importing and exporting Secure Boot signature lists as a signed binary file. This is useful to import the Microsoft revocation list binary file into the Secure Boot DBX as found on the UEFI forum at https://uefi.org/revocationlistfile.

Updated the System ROM to allow for an increased amount of 64-bit Memory Mapped I/O available for third party options cards.

Updated the System ROM support for One Button Secure Erase functionality with the latest HPE option devices.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

**Problems Fixed:**

This version of the system ROM includes updates to the Intel Memory Reference Code which may help improve memory stability for systems configured with two DIMMs per channel. Please consult Intel sighting documentation for more details on the improvements included in the Intel IPU.2.2020 release. This issue is not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigations for security vulnerabilities documented as CVE-2020-8696. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-0381. The Intel microcode patches included in this release are version 0x02006A08 (CPUID 50654), 0x04003003 (CPUID 50656) and 0x05003003 (CPUID 50567). These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS advisories and security vulnerabilities documented as CVE-2020-0587, CVE-2020-0588, CVE-2020-0590, CVE-2020-0591, CVE-2020-0592 and CVE-2020-0593. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00358. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS platform code advisories and security vulnerabilities documented as CVE-2020-8738, CVE-2020-8739, CVE-2020-8740, and CVE-2020-8764. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00390. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which addressed an issue where the system may get stuck in a reboot loop during memory training. This issue was introduced with the v2.30 System ROM. This issue was not unique to HPE servers.

Addressed an issue where the memory locality of the ACPI SLIT table was not being created properly. In rare cases, the incorrect ACPI SLIT values could cause unexpected impacts to system performance. This issue was introduced in the v2.10 version of the System ROM and was not seen with previous versions of the System ROM.

Addressed an issue where NVMe Hot-plug and Hot-add would not function properly with VMware. This issue did not impact NVMe Hot-plug or Hot-add with other operating systems.

Addressed an issue where the system would not properly call out a memory replacement event in the Integrated Management Log (IML) if an uncorrected memory failure occurred during an Advanced Double DRAM Device Correction (ADDDC) sparing operation. This fix only impacts the incorrect logging of these events and does not impact the normal operation of the system in terms of causing uncorrected memory failures or causing any change to the operation of A3DC functionality. This issue only impacts systems configured for fast Fault Tolerant Memory Mode (ADDDC).

Addressed an issue where the BIOS/Platform Configuration (RBSU) option for the Extended Memory Test could be automatically disabled after a system reboot. This issue was introduced with the v2.30 System ROM and was not seen with earlier version of the System ROM.

**Known Issues:**

None

## Fixes

**Important Notes:**

This version of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2020.2 guidance.

**Firmware Dependencies:**

None

**Problems Fixed:**

This version of the system ROM includes updates to the Intel Memory Reference Code which may help improve memory stability for systems configured with two DIMMs per channel. Please consult Intel sighting documentation for more details on the improvements included in the Intel IPU.2.2020 release. This issue is not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigations for security vulnerabilities documented as CVE-2020-8696. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-0381. The Intel microcode patches included in this release are version 0x02006A08 (CPUID 50654), 0x04003003 (CPUID 50656) and 0x05003003 (CPUID 50567). These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS advisories and security vulnerabilities documented as CVE-2020-0587, CVE-2020-0588, CVE-2020-0590, CVE-2020-0591, CVE-2020-0592 and CVE-2020-0593. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00358. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which provides mitigations for BIOS platform code advisories and security vulnerabilities documented as CVE-2020-8738, CVE-2020-8739, CVE-2020-8740, and CVE-2020-8764. These security vulnerabilities are documented in Intel Security Advisory INTEL-SA-00390. These issues are not unique to HPE servers.

This revision of the System ROM includes the latest revision of the Intel Reference Code which addressed an issue where the system may get stuck in a reboot loop during memory training. This issue was introduced with the v2.30 System ROM. This issue was not unique to HPE servers.

Addressed an issue where the memory locality of the ACPI SLIT table was not being created properly. In rare cases, the incorrect ACPI SLIT values could cause unexpected impacts to system performance. This issue was introduced in the v2.10 version of the System ROM and was not seen with previous versions of the System ROM.

Addressed an issue where NVMe Hot-plug and Hot-add would not function properly with VMware. This issue did not impact NVMe Hot-plug or Hot-add with other operating systems.

Addressed an issue where the system would not properly call out a memory replacement event in the Integrated Management Log (IML) if an uncorrected memory failure occurred during an Advanced Double DRAM Device Correction (ADDDC) sparing operation. This fix only impacts the incorrect logging of these events and does not impact the normal operation of the system in terms of causing uncorrected memory failures or causing any change to the operation of A3DC functionality. This issue only impacts systems configured for fast Fault Tolerant Memory Mode (ADDDC).

Addressed an issue where the BIOS/Platform Configuration (RBSU) option for the Extended Memory Test could be automatically disabled after a system reboot. This issue was introduced with the v2.30 System ROM and was not seen with earlier version of the System ROM.

**Known Issues:**

None

## Enhancements

Added a new BIOS/Platform Configuration (RBSU) option to Memory Options called Refresh Watermarks. When selecting the Low Watermark setting, the memory controller will help reduce susceptibility to a DDR4 RowHammer attack. It is expected that a memory performance impact will be seen when enabling the Low Watermark setting. The default operation of the system has not changed and customers wanting to provide additional RowHammer protection should enable this setting.

Added support to BIOS/Platform Configuration (RBSU) to allow importing and exporting Secure Boot signature lists as a signed binary file. This is useful to import the Microsoft revocation list binary file into the Secure Boot DBX as found on the UEFI forum at https://uefi.org/revocationlistfile.

Updated the System ROM to allow for an increased amount of 64-bit Memory Mapped I/O available for third party options cards.

Updated the System ROM support for One Button Secure Erase functionality with the latest HPE option devices.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

ROM Flash Universal Firmware Package - HPE ProLiant DL325 Gen10 Plus (A43) Servers
Version: 1.30_07-18-2020 **(Recommended)**
Filename: A43_1.30_07_18_2020.fwpkg

**Important Note!**

**Important Notes:**

None

**Deliverable Name:**

HPE ProLiant DL325 Gen10 Plus System ROM - A43

**Release Version:**

1.30_07-18-2020

**Last Recommended or Critical Revision:**

1.30_07-18-2020

**Previous Revision:**

1.26_05-11-2020

**Firmware Dependencies:**

None

**Enhancements/New Features:**

Added a new BIOS/Platform Configuration (RBSU) option for DRAM Burst Refresh Mode to provide mitigation for TRRespass and Targeted Row Refresh exploits. This option should be configured to Disabled to mitigate the TRRespass vulnerability. Setting this option to Disabled may have a minimal impact to system performance. The default setting is Enabled.

Added a new BIOS/Platform Configuration (RBSU) option in the Minimum Processor Idle Power Core C-State setting for C1 State. This option allows for power savings during certain workloads without the performance impacts of C6 State.

Added driver and option to enable SmartRAID SW RAID support for direct attached SATA drives.

**Problems Fixed:**

Addressed an issue where uncorrectable memory errors are seen when running memory intensive workloads with LRDIMMs.

Addressed an issue that could cause a slight degradation of performance.

Resolved an issue with NVMe hot add or removal which may result in an unrecoverable I/O error reported in the Integrated Management Log (IML).

Addressed an issue where the UEFI Shell command GetPciRom may not display information for PCI expansion device drivers.

Addressed an issue where the server may experience slower than expected performance when the inlet ambient temperature is greater than 30 degrees Celsius.

**Known Issues:**

None

**Fixes**

**Important Notes:**

None

**Firmware Dependencies:**

None

**Problems Fixed:**

Addressed an issue where uncorrectable memory errors are seen when running memory intensive workloads with LRDIMMs.

Addressed an issue that could cause a slight degradation of performance.

Resolved an issue with NVMe hot add or removal which may result in an unrecoverable I/O error reported in the Integrated Management Log (IML).

Addressed an issue where the UEFI Shell command GetPciRom may not display information for PCI expansion device drivers.

Addressed an issue where the server may experience slower than expected performance when the inlet ambient temperature is greater than 30 degrees Celsius.

**Known Issues:**

None

**Enhancements**

Added a new BIOS/Platform Configuration (RBSU) option for DRAM Burst Refresh Mode to provide mitigation for TRRespass and Targeted Row Refresh exploits. This option should be configured to Disabled to mitigate the TRRespass vulnerability. Setting this option to Disabled may have a minimal impact to system performance. The default setting is Enabled.

Added a new BIOS/Platform Configuration (RBSU) option in the Minimum Processor Idle Power Core C-State setting for C1 State. This option allows for power savings during certain workloads without the performance impacts of C6 State.

Added driver and option to enable SmartRAID SW RAID support for direct attached SATA drives.

---

ROM Flash Universal Firmware Package - HPE ProLiant DL385 Gen10 Plus (A42) Servers
Version: 1.30_07-18-2020 **(Recommended)**
Filename: A42_1.30_07_18_2020.fwpkg

**Important Note!**

**Important Notes:**

None

**Deliverable Name:**

HPE ProLiant DL385 Gen10 Plus System ROM - A42

**Release Version:**

1.30_07-18-2020

**Last Recommended or Critical Revision:**

1.30_07-18-2020

**Previous Revision:**

1.26_05-11-2020

**Firmware Dependencies:**

None

**Enhancements/New Features:**

Added a new BIOS/Platform Configuration (RBSU) option for DRAM Burst Refresh Mode to provide mitigation for TRRespass and Targeted Row Refresh exploits. This option should be configured to Disabled to mitigate the TRRespass vulnerability. Setting this option to Disabled may have a minimal impact to system performance. The default setting is Enabled.

Added a new BIOS/Platform Configuration (RBSU) option in the Minimum Processor Idle Power Core C-State setting for C1 State. This option allows for power savings during certain workloads without the performance impacts of C6 State.

Added driver and option to enable SmartRAID SW RAID support for direct attached SATA drives.

**Problems Fixed:**

Addressed an issue where uncorrectable memory errors are seen when running memory intensive workloads with LRDIMMs.

Addressed an issue that could cause a slight degradation of performance.

Resolved an issue with NVMe hot add or removal which may result in an unrecoverable I/O error reported in the Integrated Management Log (IML).

Addressed an issue where the UEFI Shell command GetPciRom may not display information for PCI expansion device drivers.

**Known Issues:**

None

**Fixes**

**Important Notes:**

None

**Firmware Dependencies:**

None

**Problems Fixed:**

Addressed an issue where uncorrectable memory errors are seen when running memory intensive workloads with LRDIMMs.

Addressed an issue that could cause a slight degradation of performance.

Resolved an issue with NVMe hot add or removal which may result in an unrecoverable I/O error reported in the Integrated Management Log (IML).

Addressed an issue where the UEFI Shell command GetPciRom may not display information for PCI expansion device drivers.

**Known Issues:**

None

**Enhancements**

Added a new BIOS/Platform Configuration (RBSU) option for DRAM Burst Refresh Mode to provide mitigation for TRRespass and Targeted Row Refresh exploits. This option should be configured to Disabled to mitigate the TRRespass vulnerability. Setting this option to Disabled may have a minimal impact to system performance. The default setting is Enabled.

Added a new BIOS/Platform Configuration (RBSU) option in the Minimum Processor Idle Power Core C-State setting for C1 State. This option allows for power savings during certain workloads without the performance impacts of C6 State.

Added driver and option to enable SmartRAID SW RAID support for direct attached SATA drives.

---

**Driver - Lights-Out Management** Top

HPE iLO Native Driver for ESXi 7.0
Version: 10.6.0 **(Recommended)**
Filename: ilo-driver_700.10.6.0.10-1OEM.700.1.0.15843807_16345029.zip

**Enhancements**

Support for VMware ESXi 7.0 and ESXi 7.0 U1

---

**Driver - Network** Top

HPE Blade Intel ixgben Driver for VMware vSphere 7.0
Version: 2020.06.01 **(Optional)**
Filename: cp041435.compsig; cp041435.zip

**Important Note!**

This component is intended to be used by HPE applications. It is a zip file that contains the same driver deliverable available from the vmware.com and the HPE vibsdepot.hpe.com webpages, plus an HPE specific CP0xxxxx.xml file.

HPE recommends the firmware provided in *HPE Blade Intel Online Firmware Upgrade Utility for VMware*, version 1.1.2 or later, for use with this driver.

**Enhancements**

Initial release.

**Supported Devices and Features**

These drivers support the following network adapters:

- HPE Ethernet 10Gb 2-port 560FLB Adapter
- HPE Ethernet 10Gb 2-port 560M Adapter

---

HPE Blade QLogic NX2 10/20 GbE Multifunction Driver for VMware vSphere 7.0
Version: 2020.06.01 **(Optional)**
Filename: cp041436.compsig; cp041436.zip

**Important Note!**

This component is intended to be used by HPE applications. It is a zip file that contains the same driver deliverable available from the vmware.com and the HPE vibsdepot.hp.com webpages, plus an HPE specific CP0xxxxx.xml file.

HPE recommends the firmware provided in *HPE Blade QLogic NX2 Online Firmware Upgrade Utility for VMware*, version 1.1.1 or later, for use with this driver.

**Enhancements**

Initial release.

**Supported Devices and Features**

These drivers support the following network adapters:

- HPE FlexFabric 10Gb 2-port 534M Adapter
- HPE FlexFabric 10Gb 2-port 536FLB Adapter
- HPE FlexFabric 20Gb 2-port 630FLB Adapter
- HPE FlexFabric 20Gb 2-port 630M Adapter

---

HPE Broadcom NetXtreme-E Drivers for VMware vSphere 7.0
Version: 2020.09.14 **(Optional)**
Filename: cp043308.compsig; cp043308.zip

**Important Note!**

This component is intended to be used by HPE applications. It is a zip file that contains the same driver deliverable available from the vmware.com and the HPE vibsdepot.hpe.com webpages, plus an HPE specific CP0xxxxx.xml file.

HPE recommends the firmware provided in *HPE Broadcom NetXtreme-E Online Firmware Upgrade Utility for VMware*, version 5.11.0 or later, for use with this driver.

**Enhancements**

Initial release.

**Supported Devices and Features**

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 535FLR-T Adapter
- HPE Ethernet 10Gb 2-port 535T Adapter
- HPE Ethernet 10/25Gb 2-port 631FLR-SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 631SFP28 Adapter
- HPE Ethernet 10Gb 2-port 537SFP+ Adapter
- HPE Ethernet 10Gb 2-port 537SFP+ FLR Adapter

---

HPE Intel i40en Driver for VMware vSphere 7.0
Version: 2020.05.29 **(Optional)**
Filename: cp041295.compsig; cp041295.zip

**Important Note!**

This component is intended to be used by HPE applications. It is a zip file that contains the same driver deliverable available from the vmware.com and the HPE vibsdepot.hpe.com webpages, plus an HPE specific CP0xxxxx.xml file.

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for VMware*, version 3.12.50 or later, for use with this driver.

**Enhancements**

Initial release.

**Supported Devices and Features**

This product supports the following network adapters:

- HPE Ethernet 1Gb 2-port 368FLR-MMT Adapter
- HPE Ethernet 1Gb 2-port 368i Adapter
- HPE Ethernet 1Gb 4-port 369i Adapter
- HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter
- HPE Ethernet 10Gb 2-port 562SFP+ Adapter
- HPE Ethernet 10Gb 2-port 568i Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMSFP+ Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMT Adapter

---

HPE Intel ixgben Driver for VMware vSphere 7.0
Version: 2020.05.29 **(Optional)**
Filename: cp041297.compsig; cp041297.zip

**Important Note!**

This component is intended to be used by HPE applications. It is a zip file that contains the same driver deliverable available from the vmware.com and the HPE vibsdepot.hpe.com webpages, plus an HPE specific CP0xxxxx.xml file.

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for VMware*, version 3.12.50 or later, for use with this driver.

**Enhancements**

Initial release.

**Supported Devices and Features**

These drivers support the following network adapters:

- HP Ethernet 10Gb 2-port 560FLR-SFP+ Adapter
- HP Ethernet 10Gb 2-port 560SFP+ Adapter
- HPE Ethernet 10Gb 2-port 562FLR-T Adapter
- HPE Ethernet 10Gb 2-port 562T Adapter

---

HPE QLogic FastLinQ 10/25/50 GbE Multifunction Driver for VMware vSphere 7.0
Version: 2020.10.01 **(Optional)**
Filename: cp045921.compsig; cp045921.zip

**Important Note!**

This component is intended to be used by HPE applications. It is a zip file that contains the same driver deliverable available from the vmware.com and the HPE vibsdepot.hp.com webpages, plus an HPE specific CP0xxxxx.xml file.

HPE recommends the firmware provided in *HPE QLogic FastLinQ Online Firmware Upgrade Utility for VMware*, version 4.11.50 or later, for use with this driver.

**Fixes**

Release Notes available at https://my.vmware.com/en/web/vmware/downloads/details?downloadGroup=DT-ESXI70-QLOGIC-MRVL-E4-CNA-502190&productId=974

**Supported Devices and Features**

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 521T Adapter
- HPE Ethernet 10Gb 2-port 524SFP+ Adapter
- HPE Ethernet 10/25Gb 2-port 621SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 622FLR-SFP28 Converged Network Adapter
- HPE StoreFabric CN1200R-T Converged Network Adapter
- HPE StoreFabric CN1300R Converged Network Adapter

---

HPE QLogic NX2 10/20 GbE Multifunction Driver for VMware vSphere 7.0
Version: 2020.05.29 **(Optional)**
Filename: cp041163.compsig; cp041163.zip

**Important Note!**

This component is intended to be used by HPE applications. It is a zip file that contains the same driver deliverable available from the vmware.com and the HPE vibsdepot.hp.com webpages, plus an HPE specific CP0xxxxx.xml file.

HPE recommends the firmware provided in *HPE QLogic NX2 Online Firmware Upgrade Utility for VMware*, version 1.26.50 or later, for use with this driver.

**Enhancements**

Initial release.

**Supported Devices and Features**

These drivers support the following network adapters:

- HP Ethernet 10Gb 2-port 530T Adapter
- HP Ethernet 10Gb 2-port 530SFP+ Adapter
- HPE FlexFabric 10Gb 4-port 536FLR-T Adapter
- HP FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 533FLR-T Adapter
- HPE StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R 10GBASE-T Dual Port Converged Network Adapter

---

net-mst kernel module driver component for VMware ESXi 7.0
Version: 2020.05.20 (A) **(Recommended)**
Filename: cp046234.compsig; cp046234.zip

**Important Note!**

This component is intended to be used by HPE applications. It is a zip that contains the same driver deliverable available from the HPE vibsdepot.hpe.com webpage, plus an HPE specific CPXXXX.xml file.

**Prerequisites**

NA

**Enhancements**

No Enhancement as it is Initial version.

**Supported Devices and Features**

| HPE Part Number | Device Name | PSID |
|---|---|---|
| 764282-B21 | HPE InfiniBand QDR/Ethernet 10Gb 2-port 544+M Adapter | HP_1350110023 |
| 764283-B21 | HPE InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+M Adapter | HP_1360110017 |
| 764284-B21 | HPE InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+QSFP Adapter | HP_1370110017 |
| P24837-B21 | HPE Ethernet 10/25Gb 2-port 642SFP28 Adapter | HPE0000000054 |
| P11338-B21 | HPE Ethernet 10Gb 2-port 548SFP+ Adapter | HP_1200111023 |
| 764285-B21 | HPE InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+FLR-QSFP Adapter | HP_1380110017 |
| 764286-B21 | HPE InfiniBand QDR/Ethernet 10Gb 2-port 544+FLR-QSFP Adapter | HP_1390110023 |
| 825110-B21 | HPE InfiniBand EDR/Ethernet 100Gb 1-port 840QSFP28 Adapter | HP_2180110032 |
| 825111-B21 | HPE InfiniBand EDR/Ethernet 100Gb 2-port 840QSFP28 Adapter | HP_2190110032 |
| 872726-B21 | HPE InfiniBand EDR/Ethernet 100Gb 2-port 841QSFP28 Adapter | HPE0000000009 |
| 879482-B21 | HPE InfiniBand FDR/Ethernet 40/50Gb 2-port 547FLR-QSFP Adapter | HPE0000000022 |
| 868779-B21 | HPE Synergy 6410C 25/50Gb Ethernet Adapter | HPE0000000006 |
| 779793-B21 | HPE Ethernet 10Gb 2-port 546SFP+ Adapter | HP_1200111023 |
| 779799-B21 | HPE Ethernet 10Gb 2-port 546FLR-SFP+ Adapter | HP_2240110004 |
| 817749-B21 | HPE Ethernet 25Gb 2-port 640FLR-SFP28 Adapter | HP_2690110034 |
| 817753-B21 | HPE Ethernet 25Gb 2-port 640SFP28 Adapter | HP_2420110034 |
| P21927-B21 | HPE Ethernet 100Gb 2-port QSFP28 MCX516A-CCHT Adapter | MT_0000000417 |
| P10112-B21 | HPE Ethernet 10/25Gb 2-port SFP28 MCX562A-ACAI OCP3 Adapter | MT_0000000241 |
| P13188-B21 | HPE Ethernet 10/25Gb 2-port SFP28 MCX512F-ACHT Adapter | MT_0000000416 |
| P11341-B21 | HPE Ethernet 10Gb 2-port SFP+ MCX4621A-ACAB OCP3 Adapter | MT_0000000238 |
| P21930-B21 | HPE Ethernet 10Gb 2-port SFP+ MCX4121A-XCHT Adapter | MT_0000000414 |
| P25960-B21 | HPE Ethernet 100Gb 2-Port QSFP56 MCX623106AS-CDAT Adapter | MT_0000000437 |
| 874253-B21 | HPE Ethernet 100Gb 1-port 842QSFP28 Adapter | HPE0000000014 |
| P06154-B21 | HPE InfiniBand HDR/Ethernet 200Gb 1-port 940QSFP56 x16 Adapter | HPE0000000034 |
| P06250-B21 | HPE InfiniBand HDR100/Ethernet 100Gb 1-port 940QSFP56 x16 Adapter | HPE0000000035 |
| P06251-B21 | HPE InfiniBand HDR100/Ethernet 100Gb 2-port 940QSFP56 x16 Adapter | HPE0000000036 |
| P23664-B21 | HPE InfiniBand HDR/Ethernet 200Gb 1-port MCX653105A-HDAT QSFP56 x16 Adapter | MT_0000000451 |
| P23665-B21 | HPE InfiniBand HDR100/Ethernet 100Gb 1-port MCX653105A-ECAT QSFP56 x16 Adapter | MT_0000000452 |
| P23666-B21 | HPE InfiniBand HDR100/Ethernet 100Gb 2-port MCX653106A-ECAT QSFP56 x16 Adapter | MT_0000000453 |

---

nmlx5_en Driver Component for VMware 7.0
Version: 2020.09.01 (A) **(Recommended)**
Filename: cp046896.compsig; cp046896.zip

**Important Note!**

**Known Issues in version 4.19.70.1:**

- SR-IOV is not supported while ENS is enabled.
- Live unload of the driver is not supported. Doing so may cause a PSOD if the max_vfs parameter is set.
- The maximum number of established active RDMA connections (QPs) is currently 5000.
- ENS is currently not supported in ConnectX-6 Dx adapter cards.
  **Workaround**: Use non ENS DVS for ConnectX-6 Dx cards.
- Setting ETS value to 0 may cause WQE timeout.
  **Workaround**: Set ETS value of 1 instead of 0.
- The 'esxcli mellanox uplink link info -u <vmnic_name>' command reports the 'Auto negotiation' capability always as 'true'.
- SMP MADs (ibnetdiscover, sminfo, iblinkinfo, smpdump, ibqueryerr, ibdiagnet and smpquery) are not supported on the VFs.
- Although the max_vfs module parameter range is "0-128", due to firmware limitations, the following are the supported VFs per single port devices:
  - ConnectX-4 / ConnectX-5: up to 127

**Fixes**

**No fixes are included in version 4.19.70.1:**

**Enhancements**

**No Changes and New Features are included in smart component version 2020.09.01:**

**New features and changes in version 4.19.70.1:**

- Disabled the option of shutting down the link due to power limitation.
- Support for trusting Differentiated Services Code Point (DSCP) and setting default value for RoCE traffic.
- New counter that enables the user to query per Virtual Function counters.
- RX out-of-buffer counter to indicate any lack of software receive buffers.
- support for Data Center Bridging Capability Exchange (DCBx) protocol.DCBX works with LLDP to allow switches to exchange information about their Data Center Bridging (DCB) capabilities and configuration and automatically

  negotiate common Priority-Based Flow Control (PFC) parameters.
- Module parameter to enforce specific RoCE version.
- Support for setting the minimal bandwidth guarantee for traffic classes (TCs).

**Supported Devices and Features**

| HPE Part Number | Device Name | PSID |
|---|---|---|
| 825110-B21 | HPE InfiniBand EDR/Ethernet 100Gb 1-port 840QSFP28 Adapter | HP_2180110032 |
| 825111-B21 | HPE InfiniBand EDR/Ethernet 100Gb 2-port 840QSFP28 Adapter | HP_2190110032 |
| 872726-B21 | HPE InfiniBand EDR/Ethernet 100Gb 2-port 841QSFP28 Adapter | HPE0000000009 |
| 879482-B21 | HPE InfiniBand FDR/Ethernet 40/50Gb 2-port 547FLR-QSFP Adapter | HPE0000000022 |
| 868779-B21 | HPE Synergy 6410C 25/50Gb Ethernet Adapter | HPE0000000006 |
| P11338-B21 | HPE Ethernet 10Gb 2-port 548SFP+ Adapter | HP_1200111023 |
| 817749-B21 | HPE Ethernet 25Gb 2-port 640FLR-SFP28 Adapter | HP_2690110034 |
| 817753-B21 | HPE Ethernet 25Gb 2-port 640SFP28 Adapter | HP_2420110034 |
| P24837-B21 | HPE Ethernet 10/25Gb 2-port 642SFP28 Adapter | HPE0000000054 |
| 874253-B21 | HPE Ethernet 100Gb 1-port 842QSFP28 Adapter | HPE0000000014 |
| P06154-B21 | HPE InfiniBand HDR/Ethernet 200Gb 1-port 940QSFP56 x16 Adapter | HPE0000000034 |
| P06250-B21 | HPE InfiniBand HDR100/Ethernet 100Gb 1-port 940QSFP56 x16 Adapter | HPE0000000035 |
| P06251-B21 | HPE InfiniBand HDR100/Ethernet 100Gb 2-port 940QSFP56 x16 Adapter | HPE0000000036 |

---

VMware ESXi 7.0 MST Drivers Offline Bundle for Mellanox Adapters
Version: 4.14.3.3 **(Recommended)**
Filename: Mellanox-NATIVE-NMST_4.14.3.3-1OEM.700.1.0.15525992_16211416.zip

**Prerequisites**

NA

**Enhancements**

VM70 nmst 4.14.3.3

---

**Driver - System Management** Top

HPE CRU Native Driver for ESXi 7.0
Version: 7.0.10 **(Recommended)**
Filename: cru_driver_700.10.16_1OEM.700.0.0.14828939_signed_component_15675715.zip

**Enhancements**

Support for VMware ESXi 7.0

---

**Firmware - Network** Top

Broadcom NetXtreme-E Online Firmware Upgrade Utility for VMware
Version: 5.11.6 **(Optional)**
Filename: CP043168.compsig; CP043168.zip

**Important Note!**

HPE recommends *Broadcom NetXtreme-E Drivers for VMware*, versions 216.0.54.0 or later, for use with this firmware.

This software package contains NVM Image version 216.0.333.11 with the following firmware versions:

| NIC | Bootcode Version | NCSI Version | MBA Version | UEFI Version | CCM Version | RoCE Version |
|---|---|---|---|---|---|---|
| HPE Ethernet 10/25Gb 2-port SFP28 BCM57414 OCP3 Adapter | 214.4.91.1 | 214.4.42.1 | 2214.0.241.0 | 214.0.305.0 | 216.0.52.1 | 214.0.194.0 |
| HPE Ethernet 10/25Gb 2-port SFP28 BCM57414 Adapter | | | | | | |
| HPE Ethernet 10Gb 2-port BaseT BCM57416 OCP3 Adapter | | | | | | |
| HPE Ethernet 10Gb 2-port BaseT BCM57416 Adapter | | | | | | |
| HPE Ethernet 10Gb 2-port SFP+ BCM57412 OCP3 Adapter | | | | | | |
| HPE Ethernet 10Gb 2-port SFP+ BCM57412 Adapter | | | | | | |

**Prerequisites**

This product requires the appropriate driver for your device and operating system be installed before firmware is updated.

**Enhancements**

Initial release.

**Supported Devices and Features**

This product supports the following network adapters:

- HPE Ethernet 10/25Gb 2-port SFP28 BCM57414 OCP3 Adapter
- HPE Ethernet 10Gb 2-port BaseT BCM57416 Adapter
- HPE Ethernet 10Gb 2-port BaseT BCM57416 OCP3 Adapter
- HPE Ethernet 10Gb 2-port SFP+ BCM57412 Adapter
- HPE Ethernet 10Gb 2-port SFP+ BCM57412 OCP3 Adapter

HPE Ethernet 10/25Gb 2-port SFP28 BCM57414 Adapter

---

HPE Blade QLogic NX2 Online Firmware Upgrade Utility for VMware
Version: 1.1.1 **(Optional)**
Filename: CP042923.compsig; CP042923.zip

**Important Note!**

HPE recommends the *HPE Blade QLogic NX2 10/20 GbE Multifunction Driver for VMware vSphere 7.0*, version 2020.06.01 or later, for use with this firmware.

HPE recommends the *HPE Blade QLogic NX2 10/20 GbE Multifunction Driver for VMware vSphere 6.7*, version 2019.12.20 or later, for use with this firmware.

HPE recommends the *HPE Blade QLogic NX2 10/20 GbE Multifunction Driver for VMware vSphere 6.5*, version 2019.12.20 or later, for use with this firmware.

**Prerequisites**

This product requires the appropriate driver for your device and operating system be installed before firmware is updated.

**Enhancements**

This product now supports VMware vSphere 7.0.

**Supported Devices and Features**

This product supports the following network adapters:

- HPE FlexFabric 10Gb 2-port 534M Adapter
- HPE FlexFabric 10Gb 2-port 536FLB Adapter
- HPE FlexFabric 20Gb 2-port 630FLB Adapter
- HPE FlexFabric 20Gb 2-port 630M Adapter

---

HPE Broadcom NetXtreme-E Online Firmware Upgrade Utility for VMware
Version: 5.11.6 **(Optional)**
Filename: CP043300.compsig; CP043300.zip

**Important Note!**

HPE recommends *HPE Broadcom NetXtreme-E Drivers for VMware*, versions 2020.09.14 or later, for use with this firmware.

This software package contains NVM Image version 216.0.333011 with the following firmware versions:

| NIC | Bootcode Version | NCSI Version | MBA Version | UEFI Version | CCM Version | RoCE Version |
|---|---|---|---|---|---|---|
| HPE Ethernet 10Gb 2-port 535FLR-T Adapter | 214.4.91.1 | 214.4.42.1 | 214.0.241.0 | 214.0.305.0 | 216.0.52.1 | 214.0.194.0 |
| HPE Ethernet 10Gb 2-port 535T Adapter | | | | | | |
| HPE Ethernet 10/25Gb 2-port 631FLR-SFP28 Adapter | | | | | | |
| HPE Ethernet 10/25Gb 2-port 631SFP28 Adapter | | | | | | |
| HPE Ethernet 10Gb 2-port 537SFP+ Adapter | | | | | | |
| HPE Ethernet 10Gb 2-port 537SFP+ FLR Adapter | | | | | | |

**Prerequisites**

This product requires the appropriate driver for your device and operating system be installed before firmware is updated.

**Fixes**

- This product corrects wrong names of adapters which show up while doing firmware update.
- This product corrects an issue about 2 ports in a port bond both being disconnected if we were just disconnecting 1 port.
- This product corrects an issue about LLDP nearest bridge packet not being disabled while that option under NIC HII was disabled.
- This product corrects the wrong LED behavior while attaching SFP-RJ45 tranceiver.
- This product corrects an issue about firmware not being actually updated even seeing it was reported as successfully by update utility.

**Supported Devices and Features**

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 535FLR-T Adapter
- HPE Ethernet 10Gb 2-port 535T Adapter
- HPE Ethernet 10/25Gb 2-port 631FLR-SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 631SFP28 Adapter
- HPE Ethernet 10Gb 2-port 537SFP+ Adapter
- HPE Ethernet 10Gb 2-port 537SFP+ FLR Adapter

---

HPE Broadcom NX1 Online Firmware Upgrade Utility for VMware
Version: 1.27.5 **(Optional)**
Filename: CP043297.compsig; CP043297.zip

**Important Note!**

This software package contains combo image v20.16.31 with the following firmware versions:

| NIC | Boot Code Version | PXE Version | NCSI Version | UEFI Version | CCM Version |
|---|---|---|---|---|---|
| HPE Ethernet 1Gb 2-port 330i Adapter (22BD) | 2.10 | 21.6.0 | 1.5.18 | 21.6.5 | 216.0.49.0 |
| HPE Ethernet 1Gb 4-port 331i Adapter (22BE)<br>HPE Ethernet 1Gb 4-port 331FLR Adapter | 1.46 | 21.6.0 | 1.5.18 | 21.6.5 | 216.0.49.0 |

| | | | | | |
|---|---|---|---|---|---|
| HPE Ethernet 1Gb 4-port 331T Adapter | | | | | |
| HPE Ethernet 1Gb 2-port 332i Adapter (22E8)<br>HPE Ethernet 1Gb 2-port 332T Adapter | 1.40 | 21.6.0 | 1.5.18 | 21.6.5 | 216.0.49.0 |

**Prerequisites**

This product requires the appropriate driver for your device and operating system be installed before firmware is updated.

**Fixes**

This product corrects the wrong spare number while it was originally not the same as what was written on the label of package.

**Supported Devices and Features**

This product supports the following network adapters:

- HPE Ethernet 1Gb 2-port 330i Adapter (22BD)
- HPE Ethernet 1Gb 4-port 331i Adapter (22BE)
- HPE Ethernet 1Gb 4-port 331FLR Adapter
- HPE Ethernet 1Gb 4-port 331T Adapter
- HPE Ethernet 1Gb 2-port 332i Adapter (22E8)
- HPE Ethernet 1Gb 2-port 332T Adapter

---

HPE Firmware Flash for Emulex Converged Network Adapters for VMware vSphere 7.0
Version: 2020.09.01 (b) **(Recommended)**
Filename: CP044565.compsig; CP044565.zip

**Important Note!**

Release Notes:

HPE Emulex Adapter Release Notes

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Fixed the following:

UEFI:

- HPE FlexFabric 20Gb 2-port 650FLB Adapter and HPE FlexFabric 20Gb 2-port 650M Adapter does not complete to create boot source on 2nd port

Firmware:

- Light Emiiting Diode(LED) is in invalid state when disable the port under Unified Extensible Firmware Interface (UEFI)
- Duplicate Entries found in firmware report under NIC details for few adaptors.
- Full adapter name is not displayed for HPE FlexFabric 20Gb 2-port 650M Adapter in some Rom Based Setup Utility (RBSU).
- On any HPE ProLiant server configured with the HPE Emulex XE-102 Based network adapter HPE FlexFabric 10Gb 2-port 556FLR-T Adapter with CNA (XE100 series) firmware 12.0.1110.0, 12.0.1110.10, or 12.0.1110.11 (or later), the network adapters may experience a "link down" state that is not recoverable by a power-cycle or reset.

For more details please go through the document titled "HPE ProLiant Servers Configured With Certain HPE Emulex XE-102 Based Network Adapters May Experience Link Down Due To a Firmware Issue" at the following link:https://support.hpe.com/hpesc/public/docDisplay?docId=emr_na-a00099050en_us

This Firmware package contains following firmware version:

| Adapter | Speed | Firmware |
|---|---|---|
| HPE FlexFabric 10Gb 2-port 556FLR-T Adapter | 10Gb | 12.0.1280.5 |
| HPE FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter | 10Gb | 12.0.1280.5 |
| HPE FlexFabric 20Gb 2-port 650M Adapter | 20Gb | 12.0.1280.5 |
| HPE FlexFabric 20Gb 2-port 650FLB Adapter | 20Gb | 12.0.1280.5 |
| HPE CN1200E Dual Port Converged Network Adapter | 20Gb | 12.0.1280.5 |
| HPE CN1200E-T Dual Port Adapter | 20Gb | 12.0.1280.5 |

**Prerequisites**

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

**Fixes**

Fixed the following:

UEFI:

- HPE FlexFabric 20Gb 2-port 650FLB Adapter and HPE FlexFabric 20Gb 2-port 650M Adapter does not complete to create boot source on 2nd port

Firmware:

- Light Emiiting Diode(LED) is in invalid state when disable the port under Unified Extensible Firmware Interface (UEFI)
- Duplicate Entries found in firmware report under NIC details for few adaptors.
- Full adapter name is not displayed for HPE FlexFabric 20Gb 2-port 650M Adapter in some Rom Based Setup Utility (RBSU).
- On any HPE ProLiant server configured with the HPE Emulex XE-102 Based network adapter HPE FlexFabric 10Gb 2-port 556FLR-T Adapter with CNA (XE100 series)

firmware 12.0.1110.0, 12.0.1110.10, or 12.0.1110.11 (or later), the network adapters may experience a "link down" state that is not recoverable by a power-cycle or reset.

For more details please go through the document titled "HPE ProLiant Servers Configured With Certain HPE Emulex XE-102 Based Network Adapters May Experience Link Down Due To a Firmware Issue" at the following link:https://support.hpe.com/hpesc/public/docDisplay?docId=emr_na-a00099050en_us

**Enhancements**

Updated CNA (XE100 series) firmware

**Firmware**

**Contains:**

CNA (XE100 series) firmware 12.0.1280.5

**Supported Devices and Features**

This component is supported on following Emulex Converged Network Adapters:

**XE100 Series:**

- HPE CN1200E Dual Port Converged Network Adapter
- HPE FlexFabric 20Gb 2-port 650FLB Adapter
- HPE FlexFabric 20Gb 2-port 650M Adapter
- HPE CN1200E-T Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter

---

HPE QLogic FastLinQ Online Firmware Upgrade Utility for VMware
Version: 4.12.12 **(Optional)**
Filename: CP041875.compsig; CP041875.zip

**Important Note!**

HPE recommends *HPE QLogic FastLinQ 10/25/50GbE Multifunction Drivers for VMware*, versions 2020.09.14 or later, for use with this firmware.

This software package contains combo image version v8.52.12 includes:

- Boot Code (MFW): 8.52.9.0
- UEFI: 4.1.10.2
- PXE: 2.0.19

The users will only see the combo image versions in the interactive mode firmware update or while using HPSUM/SPP to update the firmware on the supported adapters.

**Prerequisites**

This product requires the appropriate driver for your device and operating system be installed before firmware is updated.

**Fixes**

- This product corrects the abnormal disconnection of iLO web page while performing under Shared Networking on Flexible-LOM.
- This product addresses an issue where the HPE Ethernet 10/25Gb 2-port 622FLR-SFP28 adapter and HPE Ethernet 10/25Gb 2-port 621SFP28 Adapter UMCE (Uncorrectable Machine Check Exception) was followed by Unrecoverable I/O error, Uncorrectable PCI express error on Server and one of the ports suddenly no longer can send or receive traffic.
- This product addresses an issue where driver doesn't load upon booting up by correct memory relocation.
- This product addresses an issue where adapter may disappear during POST if the adapter is in heavy traffic during the system boot up.

**Enhancements**

This product improves the functionality for the MBI firmware update.

**Supported Devices and Features**

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 524SFP+ Adapter
- HPE Ethernet 10Gb 2-port 521T Adapter
- HPE Ethernet 10/25Gb 2-port 622FLR-SFP28 Converged Network Adapter
- HPE Ethernet 10/25Gb 2-port 621SFP28 Adapter
- HPE StoreFabric CN1300R Converged Network Adapter
- HPE StoreFabric CN1200R-T Converged Network Adapter

---

HPE QLogic NX2 Online Firmware Upgrade Utility for VMware
Version: 1.27.11 **(Optional)**
Filename: CP041878.compsig; CP041878.zip

**Important Note!**

HPE recommends HPE QLogic NX2 10/20GbE Multifunction Drivers for VMware, versions 2020.09.14 or later, for use with this firmware.

This software package contains combo image v7.18.69 with the following firmware versions:

| NIC | Boot Code Version | PXE Version | UEFI Version | iSCSI Version | FCoE Version | CCM Version | L2 Version |
|---|---|---|---|---|---|---|---|
| HP Ethernet 10Gb 2-port 530SFP+ Adapter<br>HP Ethernet 10Gb 2-port 530T Adapter | 7.15.77 | 7.14.13 | 8.7.2 | n/a | n/a | 7.14.4 | 7.12.25 |
| HP Ethernet 10Gb 2-port 533FLR-T Adapter<br>HP FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter<br>HPE FlexFabric 10Gb 4-port 536FLR-T Adapter<br>HP StoreFabric CN1100R Dual Port Converged Network Adapter<br>HPE StoreFabric CN1100R-T Converged Network Adapter | 7.15.77 | 7.14.13 | 8.7.2 | 7.14.0 | 7.14.3 | 7.14.4 | 7.12.25 |

**Prerequisites**

This product requires the appropriate driver for your device and operating system be installed before firmware is updated.

**Fixes**

- This product corrects the display problem of the adapter name under RBSU.
- This products corrects some issues about the thermal reporting and temperature threadshold control of the adapter.
- This product addresses an error when the MBI firmware update is executed in the secure boot mode.
- This product addresses an issue where unexpected UMCE(Uncorrectable Machine Check Exception) appeared when powering on the system with NPAR(Network Partitioning) enabled.

**Enhancements**

This product improves the functionality for the MBI firmware update.

**Supported Devices and Features**

This product supports the following network adapters:

- HP Ethernet 10Gb 2-port 530SFP+ Adapter
- HP Ethernet 10Gb 2-port 530T Adapter
- HP Ethernet 10Gb 2-port 533FLR-T Adapter
- HP FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 4-port 536FLR-T Adapter
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Converged Network Adapter

---

Marvell FastLinQ Online Firmware Upgrade Utility for VMware
Version: 4.12.14 **(Optional)**
Filename: CP042279.compsig; CP042279.zip

**Important Note!**

This software package contains combo image v8.52.21. This combo image includes:

- Boot Code (MFW): 8.52.9.0
- UEFI: 6.1.7.3

**Prerequisites**

This product requires the appropriate driver for your device and operating system be installed before firmware is updated.

**Fixes**

- This product corrects an issue of inconsistent LED behavior while linking up with different speed.
- This product corrects an issue about failing to restore the factory default value by pressing F7.
- This product addresses an issue where driver doesn't load upon booting up by correct memory relocation.
- This product addresses an issue where adapter may disappear during POST if the adapter is in heavy traffic during the system boot up.

**Enhancements**

This product now supports firmware upgrade in the ESXi 7.0.

**Supported Devices and Features**

This product supports the following network adapters:

- HPE Ethernet 10/25Gb 2-port SFP28 QL41232HQCU OCP3 Adapter
- HPE Ethernet 10/25Gb 2-port SFP28 QL41232HLCU Adapter
- HPE Ethernet 10Gb 4-port SFP+ QL41134HLCU Adapter
- HPE Ethernet 10Gb 2-port BaseT QL41132HLRJ Adapter
- HPE Ethernet 10Gb 2-port BaseT QL41132HQRJ OCP3 Adapter
- HPE Ethernet 10Gb 2-port SFP+ QL41132HQCU OCP3 Adapter
- HPE Ethernet 10Gb 2-port SFP+ QL41132HLCU Adapter

---

Online Firmware Upgrade Utility (ESXi 7.0) for HPE Ethernet 10Gb 2-port 548SFP+ Adapter
Version: 1.0.0 **(Recommended)**
Filename: CP044411.compsig; CP044411.zip

**Important Note!**

**No known issues were included in firmware version 14.27.4000:**

**Fixes**

**Following issues have been fixed in version 14.27.4000:**

- An issue that caused the sent packet to hang while the device entered FLR mode.
- Enabled Bar configuration bytewise by applying the write_en bitmask.
- A rare case where the the device froze while running the sw reset flow under heavy stress and with many open resources.
- Low PXE performance while using the VSC to trigger the send_ring_doorbells.
- An error that prevented the completions (CQ) from being completed due to a race condition in the firmware transport error handlers, and the error stressors, where the error stressors would hang the firmware transport error handler flow.
- An issue that caused the fragmented IP packets to drop was fixed.

**Enhancements**

**Firmware for the following device is updated to 14.27.4000:**

P11338-B21 (HPE Ethernet 10Gb 2-port 548SFP+ Adapter)

**Following New features and Changes are included in version 14.27.4000:**

- Added mlxconfig support for power reduction: PCI CAP AUTO_POWER_SAVE_LINK_DOWN
  - PCI CAP
  - AUTO_POWER_SAVE_LINK_DOWN
- Added the following segments, as appeared in the PRM, to the Resource Dump:
  - PRM_QUERY_QP
  - PRM_QUERY_CQ
  - PRM_QUERY_MKEY
  - QUERY_VNIC_ENV

**Supported Devices and Features**

| HPE Part Number | Mellanox Ethernet Only Adapters | PSID |
|---|---|---|
| P11338-B21 | HPE Ethernet 10Gb 2-port 548SFP+ Adapter | HPE0000000038 |

---

Online Firmware Upgrade Utility (ESXi 7.0) for HPE Mellanox Ethernet only adapters
Version: 1.0.0 **(Recommended)**
Filename: CP044390.compsig; CP044390.zip

**Important Note!**

The Firmware Upgrade Utility has been split into 2 packages for Mellanox Ethernet Only NIC adpaters, one supporting Synergy platforms and the other supporting ProLiant and Apollo platforms. This package supports Mellanox Ethernet Only NIC adapters on ProLiant and Apollo servers.

**Known Issues for FW version 2.42.5044 :**

- When using the QSFP module RTXM320-581, and performing a driver restart for the firmware upgrade/downgrade to take effect, the link does not come up.
- Enabling/disabling cq_timestamp using mlxconfig is not supported.
- In a card with 2 separate LEDs scheme (a Phy LED and a logic LED) only the Phy LED will lit. Meaning, the orange LES will not be active while the ETH link is in an idle mode.
- In SR-IOV setup, using mlxconfig when the PF is passed through to a VM requires a reboot of the Hypervisor.
- Downgrade to previous GA requires server reboot.Downgrading from v2.30.8000 or later to an earlier version than 2.30.8000 requires server reboot. Reboot the server.
- On ConnectX-3 Ethernet adapter cards, there is a mismatch between the GUID value returned by firmware management tools and that returned by fabric/driver utilities that read the GUID via device firmware (e.g., using ibstat). Mlxburn/flint return 0xffff as GUID while the utilities return a value derived from the MAC address. For all driver/firmware/software purposes, the lattervalue should be used.
- SBR should be asserted for a minimum of 50 milliseconds for the ConnectX®-3 adapters
- On Pilot1 SL230, PCIe link occasionally does not come up at Gen3 speed
- RH6.3 Inbox driver causes kernel panic when SR-IOV is enabled on VPI cards due to driver compatibility issue.
- In advanced steering mode, side band management connectivity may be lost when having more than 8 QP per mcg.
- When SR-IOV is disabled in the system BIOS, a PCI issue is noticed in Ubuntu v12.04.3 with Linux kernel v3.8 which affects NICs of several manufacturers including Mellanox's, preventing them from operating.
- MFT tools might leave the flash semaphore locked if the tool operation is forced stopped. The locked semaphore prevents the firmware from accessing the flash and causes firmware hang.
- Cable Info MAD reports a wrong cable info when usingthe MC2210411-SR4 module
- Gen2 failure at temperature sweep up to 10C/min (for MT27518A1-FDIR-BV only).
- PCIe Gen2 link unstable at temperature sweep of 10C/min for MT27518A1-FDIR-BV
- Bloom filter is currently not supported.
- Firmware downgrade message When downgrading from firmware v2.11.0000 and using MFT 3.0.0-3
- RM#DMFS should not be enabled when working with InfiniBand on MLNX_OFED-2.0.3
- RM#VPD read-only fields are writable.
- Increasing SymbolErrorCounter When working in VPI mode with port1 FDR and port2 40G, error counters misbehave and increase rapidly
- Setting the device to 128Byte CQ/EQ stride will cause misbehavior of sideband management resulting in communication loss.
- CQ and EQ cannot be configured to different stride sizes.
- ConnectX-3 Pro VF device ID is presented the same as ConnectX-3 VF device ID due to driver limitations.
- RSOD while running PXE (legacy) on G9 servers. This occurs only when PXE boot fails and BIOS boots from HDD. Currently it is pending BIOS fix.
- Changing port protocol from ETH to IB on port with NCSI/IPMI enabled while the port is connected to ETH switch is not supported.
- RDP over IPv6 is currently not functional.
- Sniffer QP cannot be removed from the regular rule after adding the QP with insertion scheme equals to “push to that rule”
- Since only a single Boot Entry Vector (BEV) per PCI Physical Function is supported, disabling the first port causes the second port to disappear as well.
- The NIC does not notify the driver of a link-down incident when a cable is unplugged from a NIC port with 56GbE port link.
- 56GbE link is not raised when using 100GbE optic cables.
- When working with MLNX_OFED v3.3-1.0.0.0, server reboot could get stuck due to a kernel panic in mlx-4_en_get_drvinfo() that is called from asynchronous event handler.
- 832298:When running ibdump, loopback traffic is mirroring into the kernel driver.
- AHS reports wrong MTU size
- RM#846523: MAC address that are set from the OS using ifconfig are not reflected in the OCBB buffer

**Known Issues for FW version 14.27.24000 and 16.27.2008:**

- When working with an NVME offload QP that is created with a unaligned page size (page_offset != 0), the QP moves to an error state on the first posted WQE.
  **Workaround**: Create an NVME offload QP with page an aligned size (page_offset = 0).
- Flow Metering capability is not functional in firmware v16.27.1016.
  **Workaround**: To use Flow Metering, use older firmware versions.
- mlxconfig query for the BOOT_INTERRUPT_DIS TLV shows a wrong value in the "current value" field.
  **Workaround**: Use "next boot" indication to see the right value.
- If Relaxed Ordering is disabled by running the "setpci" command, it will not be functional even after re-enabling it by running the "setpci" command again.
- In Socket Direct supported cards, after performing mlxfwreset, the expansion ROM register might be writable on all hosts for less than 1 second.
- quota_exceeded_command and invalid_command c

**Prerequisites**

Use iLO5 firmware version 2.30 or higher with ConnectX4/ConnectX5 firmware version 14.27.4000/16.27.2008 respectively. Thermal sensor reporting on the adapter will not be functional with older versions of iLO5 firmware.

**Fixes**

**Following issues have been fixed in firmware version 2.42.5044 :**

- An issue that prevented the firmware from detecting a link_down event thus preventing the IB bond interface from going to a failover mode.

**Following issues have been fixed in firmware version 14.27.4000:**

- The sent packet hung while the device entered FLR mode.
- Enabled Bar configuration bytewise by applying the write_en bitmask.
- The device hung while running the sw reset flow under heavy stress and with many open resources.
- The completions (CQ)completed due to a race condition in the firmware transport error handlers, and the error stressors, where the error stressors would hang the firmware transport error handler flow.
- The fragmented IP packets were dropped.

**Following issues have been fixed in firmware version 16.27.2008:**

- Although the effective BER (after FEC) was expected to meet the design targets (e.g. 10e-14 or lower), occasionally it was higher.
- High BER occured when connecting cables of type 0.5/1m DAC to an HDR speed.
- The PCIe Tx parameters did not load correctly when the speed was changed after the PCIe link was disabled.
- The desched_threshold field did not work properly.
- The "roce_adp_retrans" counter was presenting the values of the "local_ack_timeout_err" counter.
- If Relaxed Ordering was disabled by running the "setpci" command, it would not be functional even after re-enabling it by running the "setpci" command again.

**Enhancements**

**Firmware for the following devices are updated to 2.42.5044 :**

779799-B21 (HP Ethernet 10G 2-port 546FLR-SFP+ Adapter)
779793-B21 (HP Ethernet 10G 2-port 546SFP+ Adapter)

**Firmware for the following devices are updated to 14.27.4000:**

817749-B21 (HPE Ethernet 25Gb 2-port 640FLR-SFP28 Adapter)

**Firmware for the following devices are updated to 14.27.4000:**
817753-B21 (HPE Ethernet 25Gb 2-port 640SFP28 Adapter)

**Firmware for the following device is updated to 16.27.2008:**

874253-B21 (HPE Ethernet 100Gb 1-port 842QSFP28 Adapter)

**New features and changes in version 16.27.2008:**

- Added the following segments, as appeared in the PRM, to the Resource Dump:
  - PRM_QUERY_QP
  - PRM_QUERY_CQ
  - PRM_QUERY_MKEY
  - QUERY_VNIC_ENV

**New features and changes in version 14.27.4000:**

- Added mlxconfig support for power reduction:
  - PCI CAP
  - AUTO_POWER_SAVE_LINK_DOWN

**Supported Devices and Features**

| HPE Part Number | Mellanox Ethernet Only Adapters | PSID |
|---|---|---|
| 779793-B21 | HP Ethernet 10Gb 2-port 546SFP+ Adapter | HP_1200111023 |
| 779799-B21 | HP Ethernet 10Gb 2-port 546FLR-SFP+ Adapter | HP_2240110004 |
| 817749-B21 | HPE Ethernet 25Gb 2-port 640FLR-SFP28 Adapter | HP_2690110034 |
| 817753-B21 | HPE Ethernet 25Gb 2-port 640SFP28 Adapter | HP_2420110034 |
| 874253-B21 | HPE Ethernet 100Gb 1-port 842QSFP28 Adapter | HPE0000000014 |

---

Online Firmware Upgrade Utility (ESXi 7.0) for HPE Mellanox VPI (Ethernet and Infiniband mode) ConnectX4 and ConnectX5 devices on VMware ESXi 7.0
Version: 1.0.0 **(Recommended)**
Filename: CP044083.compsig; CP044083.zip

**Important Note!**

**Known Issues with firmware version 16.27.2008:**

- When working with an NVME offload QP that is created with a unaligned page size (page_offset != 0), the QP moves to an error state on the first posted WQE.
  **Workaround**: Create an NVME offload QP with page an aligned size (page_offset = 0).
- Flow Metering capability is not functional in firmware v16.27.1016.
  **Workaround**: To use Flow Metering, use older firmware versions.
- mlxconfig query for the BOOT_INTERRUPT_DIS TLV shows a wrong value in the "current value" field.
  **Workaround**: Use "next boot" indication to see the right value.
- If Relaxed Ordering is disabled by running the "setpci" command, it will not be functional even after re-enabling it by running the "setpci" command again.
- In Socket Direct supported cards, after performing mlxfwreset, the expansion ROM register might be writable on all hosts for less than 1 second.
- quota_exceeded_command and invalid_command counters do not function properly. In this firmware version, the quota_exceeded_command counter's value always remains 0, whereas the invalid_command counter increases only for some Ethernet commands failure events.

**Prerequisites**

Use iLO5 firmware version 2.30 or higher with ConnectX4/ConnectX5 firmware version 14.27.4000/16.27.2008 respectively. Thermal sensor reporting on the adapter will not be functional with older versions of iLO5 firmware.

**Fixes**

**Following issues have been fixed in firmware version 16.27.2008:**

- Although the effective BER (after FEC) was expected to meet the design targets (e.g. 10e-14 or lower), occasionally it was higher.
- High BER occured when connecting cables of type 0.5/1m DAC to an HDR speed.
- The PCIe Tx parameters did not load correctly when the speed was changed after the PCIe link was disabled.
- The desched_threshold field did not work properly.
- The "roce_adp_retrans" counter was presenting the values of the "local_ack_timeout_err" counter.
- If Relaxed Ordering was disabled by running the "setpci" command, it would not be functional even after re-enabling it by running the "setpci" command again.

**Following issues have been fixed in firmware version 12.27.4000:**

The device hung while running the sw reset flow under heavy stress and with many open resources.
- Low PXE performance observerd while using the VSC to trigger the send_ring_doorbells.
- IPoIB and DC would not work together.
- DC funtionality issues.

**Enhancements**

**Firmware for the following devices are updated to 12.27.4000:**

825110-B21 (HPE InfiniBand EDR/Ethernet 100Gb 1-port 840QSFP28 Adapter)
825111-B21 (HPE InfiniBand EDR/Ethernet 100Gb 2-port 840QSFP28 Adapter)

**New Feature and Changes in Version 12.27.4000:**

- Added the following segments, as appeared in the PRM, to the Resource Dump:
  - PRM_QUERY_QP
  - PRM_QUERY_CQ
  - PRM_QUERY_MKEY
  - QUERY_VNIC_ENV

**Firmware for the following devices are updated to 16.27.2008:**

879482-B21 (HPE InfiniBand FDR/Ethernet 40/50Gb 2-port 547FLR-QSFP Adapter)
872726-B21 (HPE InfiniBand EDR/Ethernet 100Gb 2-port 841QSFP28 Adapter)

**New Feature and Changes in Version 16.27.2008:**

**This release contains important reliability improvements and security hardening enhancements. Upgrade the firmware of the device to this release to improve the devices' firmware security and reliability.**

- Improved init_hca performance in Parallel Function initialization.

**Supported Devices and Features**

| HPE Part Number | Device Name | PSID |
|---|---|---|
| 825110-B21 | HPE InfiniBand EDR/Ethernet 100Gb 1-port 840QSFP28 Adapter | HP_2180110032 |
| 825111-B21 | HPE InfiniBand EDR/Ethernet 100Gb 2-port 840QSFP28 Adapter | HP_2190110032 |
| 872726-B21 | HPE InfiniBand EDR/Ethernet 100Gb 2-port 841QSFP28 Adapter | HPE0000000009 |
| 879482-B21 | HPE InfiniBand FDR/Ethernet 40/50Gb 2-port 547FLR-QSFP Adapter | HPE0000000022 |

---

Online Firmware Upgrade Utility (ESXi 7.0) for HPE Mellanox VPI (Ethernet and Infiniband mode) ConnectX6 devices on VMware ESXi 7.0
Version: 1.0.0 **(Recommended)**
Filename: CP044416.compsig; CP044416.zip

**Important Note!**

**ConnectX-6 VPI supports having one port as InfiniBand and the other port as Ethernet according to the following matrix of combinations.**

| **Port #2 - InfiniBand** | | | | |
|---|---|---|---|---|
| **Port #1 – Ethernet** | **HDR/HDR100** | **EDR** | **FDR** | **QDR** |
| **50GbE** | supported | not supported | not supported | supported |
| **100GbE/25GbE** | supported | not supported | not supported | supported |
| **40GbE/10GbE** | supported | not supported | not supported | supported |
| **1GbE** | supported | not supported | not supported | supported |

| **Port #2 - Ethernet** | | | | |
|---|---|---|---|---|
| **Port #1 - InfiniBand** | **50GbE** | **100GbE/25GbE** | **40GbE/10GbE** | **1GbE** |
| **HDR / HDR100** | supported | supported | not supported | supported |
| **EDR** | supported | supported | not supported | supported |
| **FDR** | not supported | not supported | not supported | not supported |
| **QDR/SDR** | supported | supported | not supported | supported |

**Prerequisites**

Use iLO5 firmware version 2.30 or higher with ConnectX6 firmware version 20.27.6008. Thermal sensor reporting on the adapter will not be functional with older versions of iLO5 firmware.

**Fixes**

**There are no new fixes in firmware version 20.27.6008.**

**Enhancements**

**Firmware for the following devices are updated to 20.27.6008:**

HPE InfiniBand HDR/Ethernet 200Gb 1-port 940QSFP56 x16 Adapter - P06154-B21
HPE InfiniBand HDR100/Ethernet 100Gb 1-port 940QSFP56 x16 Adapter - P06250-B21
HPE InfiniBand HDR100/Ethernet 100Gb 2-port 940QSFP56 x16 Adapter - P06251-B21

**New Features and Changes in Version 20.27.6008:**

- The following are the minimal software/firmware versions that support PAM4 link speeds when connected using Mellanox NIC to Mellanox Switch and Mellanox NIC to 3rd Party Switches:
  - Mellanox Onyx: 3.9.0830-038
  - ConnectX-6: 20.27.2008*

*Note: NICs with this firmware version support Mellanox-to-Mellanox connectivity with PAM4 link speeds.

- Added support for the following features:
  - Enabled KP4RS FEC on Active Fiber cable up to 30m.
  - FDR protocol.
  - Enabled updating End-to-End (E2E) credit packets instantly.

**Supported Devices and Features**

| HPE Part Number | Device Name | PSID |
|---|---|---|
| P06154-B21 | HPE InfiniBand HDR/Ethernet 200Gb 1-port 940QSFP56 x16 Adapter | HPE0000000034 |
| P06250-B21 | HPE InfiniBand HDR100/Ethernet 100Gb 1-port 940QSFP56 x16 Adapter | HPE0000000035 |
| P06251-B21 | HPE InfiniBand HDR100/Ethernet 100Gb 2-port 940QSFP56 x16 Adapter | HPE0000000036 |

---

Online Firmware Upgrade Utility (ESXi 7.0) for HPE Mellanox VPI (Ethernet and Infiniband mode) devices on VMware ESXi 7.0
Version: 1.0.0 **(Recommended)**
Filename: CP044389.compsig; CP044389.zip

**Important Note!**

**Known Issues in firmware 2.42.5000, 2.42.5056, 2.42.5700:**

- When using the  Quad Small Form-factor Pluggable (QSFP) module RTXM320-581, and performing a driver restart for the firmware upgrade/downgrade to take effect, the link does not come up.
  **Workaround**: Reboot the server.
- Enabling/disabling cq_timestamp using mlxconfig is not supported.
- In a card with 2 separate LEDs scheme (a Phy LED and a logic LED) only the Phy LED will lit. Meaning, the orange LED will not be active while the ETH link is in an idle mode.
- In SR-IOV setup, using mlxconfig when the Packet Filter (PF) is passed through to a VM requires a reboot of the Hypervisor.
- Downgrading from v2.30.8000 or later to an earlier version than 2.30.8000 requires server reboot.
  **Workaround**: Reboot the server.
- On ConnectX-3 Ethernet adapter cards, there is a mismatch between the GUID value returned by firmware management tools and that returned by fabric/ driver utilities that read the GUID via device firmware (e.g., using ibstat). Mlxburn/flint return 0xffff as GUID while the utilities return a value derived from the MAC address. For all driver/firmware/software purposes, the latter value should be used.
  **Workaround**: Please use the GUID value returned by the fabric/driver utilities (not 0xffff).
- SBR should be asserted for a minimum of 50 milliseconds for the ConnectX-3 adapters.
- On Pilot1 SL230, PCIe link occasionally does not come up at Gen3 speed.
- RHEL6.3 Inbox driver causes kernel panic when SRIOV is enabled on VPI cards due to driver compatibility issue.
- **Workaround**: Set the "do_- sense=false" parameter in the [IB_TAB] i.
- In advanced steering mode, side band management connectivity may be lost when having more than 8 QP per mcg.
- When SR-IOV is disabled in the system BIOS, a PCI issue is noticed in Ubuntu v12.04.3 with Linux kernel v3.8 which affects NICs of several manufacturers including Mellanox's, preventing them from operating.
  **Workaround**: Enable SR-IOV in the BIOS.
- Mellanox Firmware Tools (MFT) might leave the flash semaphore locked if the tool operation is forced stopped. The locked semaphore prevents the firmware from accessing the flash and causes firmware hang.
  **Workaround**: Clear the semaphore using MFT command: 'flint -clear_semaphore'
- Cable Info MAD reports a wrong cable info when using the MC2210411-SR4 module.
- Gen2 failure at temperature sweep up to 10C/min (for MT27518A1-FDIR-BV only)..
- PCIe Gen2 link unstable at temperature sweep of 10C/min for MT27518A1-FDIR-BV.
- Bloom filter is currently not supported.
- When downgrading from firmware v2.11.0000 and using MFT 3.0.0-3, the following message is displayed due to the mlxconfig tool: You are trying to override configurable FW by non-configurable FW. If you continue, old FW configurations will be cleared, do you want to continue ? (y/n) [n] : y You are trying to restore default configuration, do you want to continue ? (y/n) [n] : y.
- DMFS should not be enabled when working with InfiniBand on MLNX_OFED-2.0.3
- ConnectX®-3 Pro VF device ID is presented the same as ConnectX®-3 VF device ID due to driver limitations.
  **Workaround**: Use the physical function device ID to identify the device.
- Virtual Product Data (VPD) read-only fields are writable.
  **Workaround**: Do not write to read-only fields if you wish to preserve them.
- When working in Virtual Path Identifier (VPI) mode with port1 FDR and port2 40G, error counters misbehave and increase rapidly.
- Setting the device to 128Byte CQ/EQ stride will cause misbehavior of sideband management resulting in communication loss.
- CQ and EQ cannot be configured to different stride sizes.
- Changing port protocol from ETH to IB on port with NCSI/IPMI enabled while the port is connected to ETH switch is not supported.
  **Workaround**: 1. Unplug the cable from the switch 2. Restart driver 3. Change the protocol via the appropriate tools.
- Adapter card MCX349A-XCCN may experience longer linkup times of a few seconds with specific switches.
- Adapter card MCX349A-XCCN does not respond to ethtool “identify” command (ethtool -p/--identify).
- Remote Desktop Protocol (RDP) over IPv6 is currently not functional.
  **Workaround**: Set the default RoCE mode in the software to RoCE v2 (also when not using RoCE)
- Sniffer QP cannot be removed from the regular rule after adding the QP with insertion scheme equals to “push to that rule”.
- Since only a single Boot Entry Vector (BEV) per PCI Physical Function is supported, disabling the first port causes the second port to disappear as well.
- The NIC does not notify the driver of a link-down incident when a cable is unplugged from a NIC port with 56GbE port link.
- 56GbE link is not raised when using 100GbE optic cables.
- When working with MLNX_OFED v3.3-1.0.0.0, server reboot could get stuck due to a kernel panic in mlx4_en_get_drvinfo() that is called from asynchronous event handler.
- When running ibdump, loopback traffic is mirroring into the kernel driver.
- MAC address that are set from the OS using ifconfig are not reflected in the OCBB buffer.
- The adapter card cannot raise a 10G link vs. a 40GE capable switch port in C7000 enclosure. It can raise a 1G Link and only if the switch port allows it.
- MTUSB communication via I2C header on primary I2C bus is supported only in live-fish mode.

**Fixes**

**Fixes in version 2.42.5000:**

- PortRcvPkts counter was prevented from being cleared after resetting it.
- The system Timed Out on the configuration cycle of the Virtual Functions (VFs) when more than 10 Virtual Functions performed FLR and the completion Time Out value was configured to a range of less than 16 msec.
- The server hangs and results in NMI when running “mlxfwtop –d mt4103_pci_cr0” while restarting the driver in parallel (from a different thread). In this case, the downstream bridge over the device reported completion timeout error.
- In flow_steering, BMC could not receive a ping over IPV6 after running bmc_reboot.
- While closing the HCA, the RX packet caused bad access to resources that did not exist, and consequently caused the QPCGW or the irisc to get stuck.
- The master SMLID and the LID was either 0 or 0xFFFF when the port was neither active nor armed.
- ibdump could not capture all MADs packets.
- link did not go up after reboot.
- Fixed a rare issue that cause the PCIe configuration cycle that arrived during the time of sw_reset to generate 2 completions.
- Network Controller Sideband Interface (NC-SI) did not work when adding the disable_static_steering_ini field in the ini file, due to memory allocation issue for this field in the scratchpad.

**Fixes in version 2.42.5056:**

- Fixed an issue that resulted in reading from invalid I/O address on handover from UEFI boot to OS boot, when a port was configured as InfiniBand on a VPI adapter device.

**Enhancements**

**Firmware for the following devices are updated to 2.42.5000:**
764282-B21
764286-B21

**Firmware for the following devices are updated to 2.42.5056:**
764283-B21
764284-B21

**Firmware for the following device is updated to 2.42.5700:**
764285-B21

**New features in firmware version 2.42.5000:**

- Added support for the following features.
  - new TLV: CX3_GLOBAL_CONF to enable/disable timestamp on incoming packets through mlxconfig configuration.
  - User MAC configuration.
  - Automatically collecting mstdump before driver reset.
  - A mechanism to detect DEAD_IRISC (plastic) from TPT (iron) and raise an assert.
  - A new field is added to "set port" command which notifies the firmware what is the user_mtu size.
- Improved the debug ability for command timeout cases.

**New features and changes in firmware version 2.42.5700.**

- Modified the mlx_cmd_get_mlx_link_status command return value to return "Link Type = Ethernet" in Ethernet adapter cards.

**Supported Devices and Features**

**Supported Devices:**

| HP Part Number | Device Name | PSID |
|---|---|---|
| 764282-B21 | HP InfiniBand QDR/Ethernet 10Gb 2-port 544+M Adapter | HP_1350110023 |
| 764283-B21 | HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+M Adapter | HP_1360110017 |
| 764284-B21 | HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+QSFP Adapter | HP_1370110017 |
| 764285-B21 | HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+FLR-QSFP Adapter | HP_1380110017 |
| 764286-B21 | HP InfiniBand QDR/Ethernet 10Gb 2-port 544+FLR-QSFP Adapter | HP_1390110023 |

---

Online Firmware Upgrade Utility (ESXi 7.0) for Mellanox ConnectX6Dx Open Ethernet cards
Version: 1.0.0 **(Recommended)**
Filename: CP044406.compsig; CP044406.zip

**Important Note!**

This release contains important reliability improvements and security hardening enhancements. Upgrade the devices firmware to this release to improve the devices' firmware security and reliability.

**Known Issues in firmware 22.27.6008:**

- The CRC is being removed despite using the keep_crc flag, and the byte count of the packet are counted without the CRC.
- The port link might be unstable after phyless reset when the keep_link_up configuration is set to False, and phyless reset might be malfunction.
- When the SLTP configuration is wrongly set, the “Bad status” explanation will not be presented (only error indication) to the user.
- Modifying the Flow Control attributes during traffic might cause all packets to drop.
  **Workaround**: If such scenario took place, perform the following:
  1. Restart the driver.
  2. Stop the traffic.
  3. Change the Flow Control attributes again.
- On Dual-Port devices, and only after Rx buffer modification, resetting all Physical Functions over one port (through reboot / driver restart / FLR), while there are active Physical Functions over the second port (which caused the Rx buffer changes), will cause the Rx buffer default values to be restored, although not expected by the active Physical Function on the second port.
  **Workaround**:
  - Re-apply the changes
  - Reset the functions from both ports together (driver restart / FLRs / reboot)
  - Power cycle or reset the firmware
- After Shared Buffer modifications such as SBPR, SBPM, SBCM, the PFCC flow control modifications will override the previous Shared Buffer modifications.
  **Workaround**: Apply Shared Buffer modifications after PFCC (flow control) modifications.
- Phyless Reset is not supported when using Non-DME cables.
- Phyless Reset is not supported when using a PAM4 mode.
- When running several Phyless Reset iteration in sequence, the device may get stuck.
  **Workaround**: Run a full reset (mlxfwreset) to release it.
- Running several Phyless resets in a row might result in a race between the previous Phyless reset handling the action and the current one.
- mlxconfig query for the BOOT_INTERRUPT_DIS TLV shows a wrong value in the "current value" field.

**Workaround**: Use "next boot" indication to see the right value.
- PRBS is not functional when using Wedge switch.
- 200GbE Optical cables in Auto-Negotiation mode work only in 200GbE
- Linkup time to Wedge 100 Switch in Force mode with RS-FEC/No-FEC is 24 seconds.
- When running MH TCP, few packets are dropped every second due to no Receive WQEs.
  **Workaround**: Use 4K RX queue size: ethtool -G rx 4096
- After programing firmware in LF, power-cycle must be recovered.
- Under certain congestion conditions, where traffic packets are small, accuracy of the shared buffer configuration might not be achieved.
- Software Reset does not work on ConnectX-6 Dx adapter cards.

Note: On Adapter Firmware rewrite scenario, SUM will always discover the Mellanox Open adapter firmware smart component as applicable and select it for deployment If the server iLO5 firmware version is older than 2.30.

**Prerequisites**

Use iLO5 firmware version 2.30 or higher with ConnectX6-Dx firmware version 22.27.6008. Thermal sensor reporting on the adapter will not be functional with older versions of iLO5 firmware.

**Fixes**

**Following issues have been resolved in firmware version 22.27.6008:**

- Encapsulated RoCE traffic to drop when IB padding was required.
- PortXmitWait HW counter to count when not expected due to an inaccuracy in the counter.
- On dual-port device after Rx buffer modification the Physical Function on the second port got restored although no expected. The Rx buffer changes when all Physical Functions resets over one port (through reboot /driver restart / FLR) while there were active Physical Functions over the second port.
- Previous Shared Buffer modifications being overrun after performing Shared Buffer modifications such as SBPR, SBPM, SBCM, the PFCC Flow Control).

**Enhancements**

**Firmware for the following device is updated to 22.27.6008:**

P25960-B21 (HPE Ethernet 100Gb 2-Port QSFP56 MCX623106AS-CDAT Adapter)

**New features and changes in version 22.27.6008:**

- The following are the minimal software/firmware versions that support PAM4 link speeds when connected using Mellanox NIC to Mellanox Switch and Mellanox NIC to 3rd Party Switches:
  - Mellanox Spectrum-3: 30.2007.1142
  - Mellanox Spectrum-2: 29.2007.1142
  - Switch SDK: 4.4.0920
  - Mellanox Onyx: 3.9.0830-038
  - SONiC/SAI: 201911
  - ConnectX-6 Dx: 22.27.2008

  *Note: NICs with this firmware version support Mellanox-to-Mellanox connectivity with PAM4 link speeds.
- Programmable Congestion Control (PCC) is at GA level.
- Enabled TLS offload v1.3 with key size 256.

**Supported Devices and Features**

| HPE Part Number | Mellanox Ethernet Only Adapters | PSID |
|---|---|---|
| P25960-B21 | HPE Ethernet 100Gb 2-Port QSFP56 MCX623106AS-CDAT Adapter | MT_0000000437 |

---

Online Firmware Upgrade Utility (ESXi 7.0) for Mellanox Open Ethernet cards
Version: 1.0.0 **(Recommended)**
Filename: CP044391.zip; CP044391_part1.compsig; CP044391_part2.compsig

**Important Note!**

**Known Issues in firmware 14.27.4000:**

- “mlxconfig” query for the BOOT_INTERRUPT_DIS TLV shows a wrong value in the "current value" field.
- Due to the string DB not being updated after Live-Patch, the tracer cannot function after Live-Patch.
- Hardware arbitration is currently disabled in OCP3.0 cards. It will be supported on future releases for the same hardware.
- Since Packet Pacing enforce max_tc value is “1”, features that require multiple TCs will not be active when this mode is available.
- Due to performance considerations, unicast loopback traffic will go through the NIC SX tables, and multicast loopback traffic will skip the NIC SX tables

**Known Issues with firmware version 16.27.2008:**

- When working with an NVME offload QP that is created with a unaligned page size (page_offset != 0), the QP moves to an error state on the first posted WQE.
  **Workaround**: Create an NVME offload QP with page an aligned size (page_offset = 0).
- Flow Metering capability is not functional in firmware v16.27.1016.
  **Workaround**: To use Flow Metering, use older firmware versions.
- mlxconfig query for the BOOT_INTERRUPT_DIS TLV shows a wrong value in the "current value" field.
  **Workaround**: Use "next boot" indication to see the right value.
- If Relaxed Ordering is disabled by running the "setpci" command, it will not be functional even after re-enabling it by running the "setpci" command again.
- In Socket Direct supported cards, after performing mlxfwreset, the expansion ROM register might be writable on all hosts for less than 1 second.
- quota_exceeded_command and invalid_command counters do not function properly. In this firmware version, the quota_exceeded_command counter’s value always remains 0, whereas the invalid_command counter increases only for some Ethernet commands failure events.

Note: On Adapter Firmware rewrite scenario, SUM will always discover the Mellanox Open adapter firmware smart component as applicable and select it for deployment If the server iLO5 firmware version is older than 2.30.

**Prerequisites**

Use iLO5 firmware version 2.30 or higher with ConnectX4/ConnectX5 firmware version 14.27.4000/16.27.2008 respectively. Thermal sensor reporting on the adapter will not be functional with older versions of iLO5 firmware.

**Fixes**

**Following issues have been fixed in firmware version 16.27.2008:**

- Although the effective BER (after FEC) was expected to meet the design targets (e.g. 10e-14 or lower), occasionally it was higher.

- High BER occured when connecting cables of type 0.5/1m DAC to an HDR speed.
- The PCIe Tx parameters did not load correctly when the speed was changed after the PCIe link was disabled.
- The desched_threshold field did not work properly.
- The "roce_adp_retrans" counter was presenting the values of the "local_ack_timeout_err" counter.
- If Relaxed Ordering was disabled by running the "setpci" command, it would not be functional even after re-enabling it by running the "setpci" command again.

**Following issues have been fixed in firmware version 14.27.4000:**

- The device hung while running the sw reset flow under heavy stress and with many open resources.
- Low PXE performance observerd while using the VSC to trigger the send_ring_doorbells.
- IPoIB and DC would not work together.
- DC funtionality issues.

**Enhancements**

**Firmware for the following devices is updated to 14.27.4000:**

P21930-B21 (HPE Ethernet 10Gb 2-port SFP+ MCX4121A-XCAT Adapter)
P11341-B21 (HPE Ethernet 10Gb 2-port SFP+ MCX4621A-ACAB OCP3 Adapter)

**Firmware for the following devices is updated to 16.27.2008:**

P13188-B21 (HPE Ethernet 10/25Gb 2-port SFP28 MCX512F-ACAT Adapter)
P21927-B21 (HPE Ethernet 100Gb 2-Port QSFP28 MCX516A-CCHT Adapter)
P10112-B21 (HPE Ethernet 10/25Gb 2-port SFP28 MCX562A-ACAI OCP3 Adapter)

**New Feature and Changes in Version 14.27.4000:**

- Added the following segments, as appeared in the PRM, to the Resource Dump:
  - PRM_QUERY_QP
  - PRM_QUERY_CQ
  - PRM_QUERY_MKEY
  - QUERY_VNIC_ENV

**New Feature and Changes in Version 16.27.2008:**

**This release contains important reliability improvements and security hardening enhancements. Upgrade the firmware of the device to this release to improve the devices' firmware security and reliability.**

- Improved init_hca performance in Parallel Function initialization.

**Supported Devices and Features**

| HPE Part Number | Mellanox Ethernet Only Adapters | PSID |
|---|---|---|
| P21930-B21 | HPE Ethernet 10Gb 2-port SFP+ MCX4121A-XCHT Adapter | MT_0000000414 |
| P11341-B21 | HPE Ethernet 10Gb 2-port SFP+ MCX4621A-ACAB OCP3 Adapter | MT_0000000238 |
| P13188-B21 | HPE Ethernet 10/25Gb 2-port SFP28 MCX512F-ACHT Adapter | MT_0000000416 |
| P10112-B21 | HPE Ethernet 10/25Gb 2-port SFP28 MCX562A-ACAI OCP3 Adapter | MT_0000000241 |
| P21927-B21 | HPE Ethernet 100Gb 2-port QSFP28 MCX516A-CCHT Adapter | MT_0000000417 |

---

Online Firmware Upgrade Utility (ESXi 7.0) for Mellanox Open VPI (Ethernet and Infiniband mode) ConnectX6 devices on VMware ESXi 7.0
Version: 1.0.0 **(Recommended)**
Filename: CP044420.compsig; CP044420.zip

**Important Note!**

**ConnectX-6 VPI supports having one port as InfiniBand and the other port as Ethernet according to the following matrix of combinations.**

| Port #2 - InfiniBand | | | | |
|---|---|---|---|---|
| **Port #1 – Ethernet** | **HDR/HDR100** | **EDR** | **FDR** | **QDR** |
| **50GbE** | supported | not supported | not supported | supported |
| **100GbE/25GbE** | supported | not supported | not supported | supported |
| **40GbE/10GbE** | supported | not supported | not supported | supported |
| **1GbE** | supported | not supported | not supported | supported |

| Port #2 - Ethernet | | | | |
|---|---|---|---|---|
| **Port #1 - InfiniBand** | **50GbE** | **100GbE/25GbE** | **40GbE/10GbE** | **1GbE** |
| **HDR / HDR100** | supported | supported | not supported | supported |
| **EDR** | supported | supported | not supported | supported |
| **FDR** | not supported | not supported | not supported | not supported |
| **QDR/SDR** | supported | supported | not supported | supported |

Note: On Adapter Firmware rewrite scenario, SUM will always discover the Mellanox Open adapter firmware smart component as applicable and select it for deployment if the server iLO5 firmware version is older than 2.30.

**Prerequisites**

Use iLO5 firmware version 2.30 or higher with ConnectX5/ConnectX6 firmware version 20.27.6008. Thermal sensor reporting on the adapter will not be functional with older versions of iLO5 firmware.

**Fixes**

**The following issues have been fixed in version 20.27.6008:**

- Enabled Bar configuration bytewise by applying the write_en bitmask.
- Low PXE performance while using the VSC to trigger the send_ring_doorbells.
- Fragmented IP packets were getting dropped.
- Firmware burning after PHY-less reset is expected to be significantly slow.
- PortCounters.PortRcvErr / PPCNT.infiniband_counters.PortRcvErr were not reporting port icrc errors.
- PortXmitWait HW counter was incrementing when not expected due to an inaccuracy in the counter.

**Enhancements**

**Firmware for the following devices are updated to 20.27.6008:**

- HPE InfiniBand HDR/Ethernet 200Gb 1-port MCX653105A-HDAT QSFP56 x16 Adapter - P23664-B21
- HPE InfiniBand HDR100/Ethernet 100Gb 1-port MCX653105A-ECAT QSFP56 x16 Adapter - P23665-B21
- HPE InfiniBand HDR100/Ethernet 100Gb 2-port MCX653106A-ECAT QSFP56 x16 Adapter - P23666-B21

**New Features and Changes in Version 20.27.6008:**

- The following are the minimal software/firmware versions that support PAM4 link speeds when connected using Mellanox NIC to Mellanox Switch and Mellanox NIC to 3rd Party Switches:
  - Mellanox Onyx: 3.9.0830-038
  - ConnectX-6: 20.27.2008*
    *Note: NICs with this firmware version support Mellanox-to-Mellanox connectivity with PAM4 link speeds.
- Added support for the following features:
  - Enabled KP4RS FEC on Active Fiber cable up to 30m.
  - FDR protocol.
  - Enabled updating End-to-End (E2E) credit packets instantly.

**Supported Devices and Features**

| HPE Part Number | Device Name | PSID |
|---|---|---|
| P23664-B21 | HPE InfiniBand HDR/Ethernet 200Gb 1-port MCX653105A-HDAT QSFP56 x16 Adapter | MT_0000000451 |
| P23665-B21 | HPE InfiniBand HDR100/Ethernet 100Gb 1-port MCX653105A-ECAT QSFP56 x16 Adapter | MT_0000000452 |
| P23666-B21 | HPE InfiniBand HDR100/Ethernet 100Gb 2-port MCX653106A-ECAT QSFP56 x16 Adapter | MT_0000000453 |

---

**Firmware - NVDIMM** Top

Firmware Package - 16GB NVDIMM-N DDR4-2666
Version: 1.04 (B) **(Recommended)**
Filename: nvdimm-16gb_1.04.fwpkg

**Enhancements**

This product now supports Microsoft Windows Server 2019, Red Hat Enterprise Linux 8, SUSE Linux Enterprise Server 15 and VMware ESXi 7.0.

**Supported Devices and Features**

This package supports the following Memory Device:

- HPE 16GB NVDIMM Single Rank x4 DDR4-2666 Module Kit

---

Firmware package for HPE Persistent Memory featuring Intel Optane DC Persistent Memory on HPE Gen10 Servers
Version: 01.02.00.5435 (B) **(Recommended)**
Filename: dcpmm_01.02.00.5435.fwpkg

**Important Note!**

This software package contains Intel Optane DC Persistent Memory Firmware version 1.2.0.5435

**Enhancements**

- This product contains mainly performance improvements.
- This product now supports Red Hat Enterprise Linux 8, SUSE Linux Enterprise Server 12 and VMware ESXi 7.0.

**Supported Devices and Features**

This package supports the following Memory Devices:

- HPE 512GB 2666 Persistent Memory Kit featuring Intel Optane DC Persistent Memory
- HPE 256GB 2666 Persistent Memory Kit featuring Intel Optane DC Persistent Memory
- HPE 128GB 2666 Persistent Memory Kit featuring Intel Optane DC Persistent Memory

---

Online Flash Component for Linux - 16GB NVDIMM-N DDR4-2666
Version: 1.04 (B) **(Optional)**
Filename: RPMS/x86_64/firmware-nvdimm-16gb-1.04-2.1.x86_64.compsig; RPMS/x86_64/firmware-nvdimm-16gb-1.04-2.1.x86_64.rpm

**Fixes**

Initial release.

**Enhancements**

This product now supports Red Hat Enterprise Linux 8, SUSE Linux Enterprise Server 15 and VMware ESXi 7.0.

**Supported Devices and Features**

This package supports the following Memory Device:

- HPE 16GB NVDIMM Single Rank x4 DDR4-2666 Module Kit

---

**Firmware - Storage Controller** Top

HPE D3600/D3700/D3610/D3710 12Gb SAS Disk Enclosure ROM Flash Component for VMware (ESXi)
Version: 5.04 (A) **(Recommended)**
Filename: CP044974.compsig; CP044974.md5; CP044974.zip

**Important Note!**

**IMPORTANT:** Firmware updates must be performed during a system maintenance window, with all I/O to the system halted. In single domain configuration, if user hosts an OS in D3000(or any storage box) and flash the SEPs, it will hang/crash everytime as SmartComponent will reset the SEPs after flash/codeload.

**WARNING!** Do not power cycle or restart during the firmware update as this can result in loss of capabilities for this unit. It typically takes several minutes for the firmware to load.

**NOTE:** All firmware flash progress messages are logged to /var/cpq/D3000.log and flash summary is logged to /var/cpq/Component.log.

**Prerequisites**

IMPORTANT: Firmware updates must be performed during a system maintenance window, with all I/O to the system halted.

WARNING! Do not power cycle or restart during the firmware update as this can result in loss of capabilities for this unit. It typically takes several minutes for the firmware to load.

NOTE: All firmware flash progress messages are logged to /var/cpq/D3000.log and flash summary is logged to /var/cpq/Component.log.

**Fixes**

**The following fixes were incorporated in this version:**

- The Enabled-ClusterS2D command now completes successfully when executed on a SATA drive within a D3610 disk enclosure for a NonStop solution.
- The smart carrier, which is the drive case for SAS drives, now authenticates in the D3610/D3710 drive enclosure.
- Added new 7-segment error codes E0 and E1 to report issues with Fan modules A and B, respectively. These new codes only apply to the D3610/D3710 and only display when running firmware 5.04.
- If the storage enclosure processor within the I/O module fails, a hard reset (power down and then power up) is executed to ensure the processor comes back online.

Please refer to the Release Notes for the complete listing of fixes, enhancements, known issues and work-arounds corresponding to this firmware.

**Supported Devices and Features**

The D3600 / D3700 / D3610 / D3710 Enclosure can be attached to any of the following HPE Storage Controllers and Host Bus Adapters :

- Smart Array P408e-p Controller
- Smart Array E208e-p Controller
- Smart Array P408e-m Controller

---

HPE D6020 12Gb SAS Disk Enclosure ROM Flash Component for VMware (ESXi)
Version: 2.74 (H) **(Recommended)**
Filename: CP044572.compsig; CP044572.md5; CP044572.zip

**Important Note!**

**IMPORTANT:** Firmware updates must be performed during a system maintenance window, with all I/O to the system halted. In single domain configuration, if user hosts an OS in D6020(or any storage box) and flash the SEPs, it will hang/crash everytime as SmartComponent will reset the SEPs after flash/codeload.

**WARNING!** Do not power cycle or restart during the firmware update as this can result in loss of capabilities for this unit. It typically takes several minutes for the firmware to load.

**NOTE:** All firmware flash progress messages are logged to /var/cpq/D6020.log and flash summary is logged to /var/cpq/Component.log.

**Prerequisites**

IMPORTANT: Firmware updates must be performed during a system maintenance window, with all I/O to the system halted.

WARNING! Do not power cycle or restart during the firmware update as this can result in loss of capabilities for this unit. It typically takes several minutes for the firmware to load.

NOTE: All firmware flash progress messages are logged to /var/cpq/D6020.log and flash summary is logged to /var/cpq/Component.log.

**Fixes**

**The following fixes were incorporated in this version:**

- Temperature sensors logic inside gSEP model and SES database
- When an IOM is pulled the surviving IOM reports false critical temperatures

Please refer to the Release Notes for the complete listing of fixes, enhancements, known issues and work-arounds corresponding to this firmware.

**Supported Devices and Features**

The D6020 Enclosure can be attached to any of the following HPE Storage Controllers and Host Bus Adapters :

- Smart Array P408e-p Controller
- Smart Array E208e-p Controller
- Smart Array P408e-m Controller

---

HPE D8000 12Gb SAS Disk Enclosure ROM Flash Component for VMware (ESXi)
Version: 0107 (A) **(Recommended)**
Filename: CP044975.compsig; CP044975.md5; CP044975.zip

**Important Note!**

**IMPORTANT:** Firmware updates must be performed during a system maintenance window, with all I/O to the system halted. In single domain configuration, if user hosts an OS in D8000(or any storage box) and flash the SEPs, it will hang/crash everytime as SmartComponent will reset the SEPs after flash/codeload.

**WARNING!** Do not power cycle or restart during the firmware update as this can result in loss of capabilities for this unit. It typically takes several minutes for the firmware to load.

**NOTE:** All firmware flash progress messages are logged to /var/cpq/D8000.log and flash summary is logged to /var/cpq/Component.log.

**Prerequisites**

IMPORTANT: Firmware updates must be performed during a system maintenance window, with all I/O to the system halted.

WARNING! Do not power cycle or restart during the firmware update as this can result in loss of capabilities for this unit. It typically takes several minutes for the firmware to load.

NOTE: All firmware flash progress messages are logged to /var/cpq/D8000.log and flash summary is logged to /var/cpq/Component.log.

**Fixes**

**The following fixes were incorporated in this version:**

- In STD INQUIRY RESPONSE, the ErrM bit was always being set. The ErrM bit indicates that the enclosure firmware detects a mismatch in any of its package versions and the firmware version of a FRU component. The issue was due to an incorrect version of PSU firmware being included and that has been fixed.
- After installing the latest firmware on the enclosure I/O modules, the SES targets could not be discovered on the host. The virtual phy bit in SMP DISCOVER RESPONSE, which is used by the Microchip smartpqi HBA, was det for the virtual phy of the I/O module.

Please refer to the Release Notes for the complete listing of fixes, enhancements, known issues and work-arounds corresponding to this firmware.

**Supported Devices and Features**

The D8000 Enclosure can be attached to any of the following HPE Storage Controllers and Host Bus Adapters :

- HPE Smart Array P408e-p Controller
- HPE Smart Array E208e-p Controller

---

Online Firmware Flash for ESXi - HPE NS204i-p Gen10+ Boot Controller
Version: 1.0.14.1047 **(Recommended)**
Filename: CP041687.compsig; CP041687.zip

**Important Note!**

VMware **7.0u1 is** supported by HPE NS204i-p Gen10+ Boot Controller

**VMware 7.0 is NOT supported by HPE NS204i-p Gen10+ Boot Controller**

**Prerequisites**

Requires iLO5 version 2.30 or later

For Intel Gen10 systems, requires system BIOS 2.36 or later.
For AMD Gen10 Plus systems, requires system BIOS 1.30 or later.

**Enhancements**

- Initial Firmware Smart Component release for HPE Gen10+ Boot Controller

---

Online ROM Flash Component for ESXi (x86) - HPE Smart Array P824i-p MR Gen10
Version: 24.23.0-0043 (B) **(Recommended)**
Filename: CP044443.compsig; CP044443.zip

**Enhancements**

Added support for VMware ESXi 7.0

---

Online ROM Flash Component for VMware ESXi - HPE Apollo 2000 Gen10 Backplane Expander Firmware
Version: 1.00 (E) **(Recommended)**
Filename: CP044326.compsig; CP044326.zip

**Important Note!**

Customers who already installed firmware version 1.00 do not need to update to 1.00 (E).

**Enhancements**

Added VMware ESXi 7.0 support

---

Online ROM Flash Component for VMware ESXi - HPE Apollo 45xx Gen10 Backplane Expander Firmware
Version: 1.56 (F) **(Recommended)**
Filename: CP044312.compsig; CP044312.zip

**Enhancements**

- Added VMware ESXi 7.0 Support

---

Online ROM Flash Component for VMware ESXi - HPE SAS Expander Firmware for HPE D2500sb Storage Blade
Version: 2.02 (A) **(Recommended)**
Filename: CP044325.compsig; CP044325.zip

**Important Note!**

When using ESXi6.0 you must be at upgrade 3 or newer. The required SmartPQI driver is not present in earlier versions of the OS

**Prerequisites**

When using ESXi6.0 you must be at upgrade 3 or newer. The required SmartPQI driver is not present in earlier versions of the OS

**Enhancements**

Added ESXi 7.0 support.

---

**Firmware - Storage Fibre Channel** Top

HPE Firmware Flash for Emulex Fibre Channel Host Bus Adapters for VMware vSphere 7.0
Version: 2020.09.01 **(Recommended)**
Filename: CP042544.compsig; CP042544.zip

**Important Note!**

Release Notes:

HPE Emulex Adapter Release Notes

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

This Firmware package contains following firmware versions:

| Adapter | Speed | Universal Boot Image | Firmware | UEFI | Boot Bios |
|---|---|---|---|---|---|
| HPE 81E 8Gb Single Port PCIe Fibre Channel Host Bus Adapter | 8Gb | 12.60a4 | 2.10X6 | 12.6.284.0 | 12.6.302.0 |
| HPE 82E 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter | 8Gb | 12.60a4 | 2.10X6 | 12.6.284.0 | 12.6.302.0 |
| HPE 84E 8Gb Quad Port Fibre Channel Host Bus Adapter | 8Gb | 12.60a4 | 2.10X6 | 12.6.284.0 | 12.6.302.0 |
| HPE SN1000E 16Gb Dual Port Fibre Channel Host Bus Adapter | 16Gb | 12.6.275.12 | 12.6.275.12 | 12.6.275.7 | 12.6.271.0 |
| HPE SN1000E 16Gb Single Port Fibre Channel Host Bus Adapter | 16Gb | 12.6.275.12 | 12.6.275.12 | 12.6.275.7 | 12.6.271.0 |
| HPE SN1100E 16Gb Dual Port Fibre Channel Host Bus Adapter | 16Gb | 12.6.275.12 | 12.6.275.12 | 12.6.275.7 | 12.6.271.0 |
| HPE SN1100E 16Gb Single Port Fibre Channel Host Bus Adapter | 16Gb | 12.6.275.12 | 12.6.275.12 | 12.6.275.7 | 12.6.271.0 |
| HPE SN1100E Quad Port 16Gb Fibre Channel Host Bus Adapter | 16Gb | 12.6.275.12 | 12.6.275.12 | 12.6.275.7 | 12.6.271.0 |
| HPE SN1200E 16Gb Dual Port Fibre Channel Host Bus Adapter | 16Gb | 12.6.275.12 | 12.6.275.12 | 12.6.275.7 | 12.6.271.0 |
| HPE SN1200E 16Gb Dual Port Fibre Channel Host Bus Adapter | 16Gb | 12.6.275.12 | 12.6.275.12 | 12.6.275.7 | 12.6.271.0 |
| HPE SN1200E 16Gb Single Port Fibre Channel Host Bus Adapter | 16Gb | 12.6.275.12 | 12.6.275.12 | 12.6.275.7 | 12.6.271.0 |
| HPE SN1600E 32Gb Dual Port Fibre Channel Host Bus Adapter | 32Gb | 12.6.275.12 | 12.6.275.12 | 12.6.275.7 | 12.6.271.0 |
| HPE SN1600E 32Gb Single Port Fibre Channel Host Bus Adapter | 32Gb | 12.6.275.12 | 12.6.275.12 | 12.6.275.7 | 12.6.271.0 |
| HPE SN1610E 32Gb Single Port Fibre Channel Host Bus Adapter | 32Gb | 12.6.275.12 | 12.6.275.12 | 12.6.275.7 | 12.6.271.0 |
| HPE SN1610E 32Gb Dual Port Fibre Channel Host Bus Adapter | 32Gb | 12.6.275.12 | 12.6.275.12 | 12.6.275.7 | 12.6.271.0 |

**Prerequisites**

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

**Enhancements**

We have separate components to update fibre channel and converged network adapters. This is a fibre channel update component.

**Contains:**

32 Gb universal boot 12.6.275.12(EFI 12.6.275.7 BOOT BIOS 12.6.271.0 Firmware 12.6.275.12)

16/32 Gb universal boot 12.6.275.12(EFI 12.6.275.7 BOOT BIOS 12.6.271.0 Firmware 12.6.275.12)

16 Gb universal boot 12.6.275.12(EFI 12.6.275.7 BOOT BIOS 12.6.271.0 Firmware 12.6.275.12)

8 Gb HBA Standup firmware 2.10X6
8 Gb standup universal boot image 12.60a4(12.6.302.0 BIOS, 12.6.284.0 UEFI)

**Supported Devices and Features**

This component is supported on following Emulex Fibre Channel Host Bus adapters:

**8Gb FC Adapter:**

- HPE 81E 8Gb Single Port PCIe Fibre Channel Host Bus Adapter
- HPE 82E 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter
- HPE 84E 8Gb Quad Port Fibre Channel Host Bus Adapter

**16Gb FC Adapter:**

- HPE SN1000E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HPE SN1000E 16Gb Single Port Fibre Channel Host Bus Adapter
- HPE SN1100E 16Gb Dual Port Fibre Channel Host Bus Adapter

- HPE SN1100E 16Gb Single Port Fibre Channel Host Bus Adapter
- HPE SN1100E Quad Port 16Gb Fibre Channel Host Bus Adapter
- HPE SN1200E 16Gb Dual Port  Fibre Channel Host Bus Adapter
- HPE SN1200E 16Gb 1Single Port Fibre Channel Host Bus Adapter

**32Gb FC Adapter:**

- HPE SN1600E 32Gb Dual Port Fibre Channel Host Bus Adapter
- HPE SN1600E 32Gb Single Port Fibre Channel Host Bus Adapter
- HPE SN1610E 32Gb Dual port Fibre Channel Host Bus Adapter
- HPE SN1610E 32Gb Single port Fibre Channel Host Bus Adapter

---

HPE Firmware Flash for Emulex Mezzanine Fibre Channel Host Bus Adapters for VMware vSphere 7.0
Version: 2020.09.01 **(Recommended)**
Filename: CP042545.compsig; CP042545.zip

**Important Note!**

Release Notes:

HPE Emulex Adapter Release Notes

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

This Firmware package contains following firmware versions:

| Adapter | Speed | Universal Boot Image | Firmware | UEFI | Boot Bios |
|---|---|---|---|---|---|
| HPE LPe1205A 8Gb Fibre Channel Host Bus Adapter for BladeSystem c-Class | 8Gb | 12.40a6 | 2.10X6 | 12.4.262.0 | 12.4.153.0 |
| HPE 16Gb LPe1605 Fibre Channel Host Bus Adapter for BladeSystem c-Class | 16Gb | 12.4.270.10 | 12.4.270.10 | N/A | N/A |

**Prerequisites**

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

**Enhancements**

We  have separate components to update fibre channel and converged network adapters. This is a fibre channel update component.

**Contains:**

16 Gb universal boot 12.4.270.10

8 Gb Gen8 Mezz (LPe1205A) firmware 2.10X6
8 Gb Mezz universal boot image 12.40a6(12.4.262.0 BIOS, 12.4.153.0 UEFI)

**Supported Devices and Features**

This component is supported on following Emulex Fibre Channel Host Bus adapters:

**8Gb FC Adapter:**

- HPE LPe1205A 8Gb Fibre Channel Host Bus Adapter for BladeSystem c-Class

**16Gb FC Adapter:**

- HPE  LPe1605 16Gb Fibre Channel Host Bus Adapter for BladeSystem c-Class

---

HPE Firmware Flash for QLogic Fibre Channel Host Bus Adapters for VMware vSphere 7.0
Version: 2020.09.01 **(Recommended)**
Filename: CP042547.compsig; CP042547.zip

**Important Note!**

Refer release notes available at:

HPE QLogic Adapter Release Notes

This Firmware package contains following firmware versions:

| Adapter | Speed | MBI | Firmware | UEFI | Boot Bios |
|---|---|---|---|---|---|
| HPE 81Q 8Gb PCIe Fibre Channel Host Bus Adapter | 8Gb | 3.82.00 | 8.08.207 | 7.00 | 3.56 |
| HPE 82Q 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter | 8Gb | 3.82.00 | 8.08.207 | 7.00 | 3.56 |
| HPE 84Q 8Gb Quad Port Fibre Channel Host Bus Adapter | 8Gb | 3.82.00 | 8.08.207 | 7.00 | 3.56 |
| HPE SN1000Q 16GB Dual Port PCIe Fibre Channel Host Bus Adapter | 16Gb | 6.03.00 | 8.08.231 | 7.02 | 3.43 |
| HPE SN1000Q 16GB Single Port PCIe Fibre Channel Host Bus Adapter | 16Gb | 6.03.00 | 8.08.231 | 7.02 | 3.43 |

| | | | | | |
|---|---|---|---|---|---|
| HPE SN1610Q 32Gb Dual Port Fibre Channel Host Bus Adapter | 32Gb | 02.03.06 | 09.04.01 | 7.08 | 0.0 |
| HPE SN1610Q 32Gb Single Port Fibre Channel Host Bus Adapter | 32Gb | 02.03.06 | 09.04.01 | 7.08 | 0.0 |

Fixed the following:

- Enhancements have been made to the firmware to prevent and better recover from the unexpected behavior described in Customer Advisory titled: “HPE ProLiant, Synergy and Superdome Flex Host Bus Adapters (HBA) - Certain Fibre Channel HBA Firmware May Cause the Operating System to Halt and Potentially Compromise Filesystem Data Integrity" at the following link:

  https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=a00094722en_us

- Address unexpected behavior when Fibre Channel adapters were simultaneously running traffic to an array which supports 3PAR Persistent Checksum AND another array which is running T10-PI (also known as T10-DIF) or no block checksum technology at all
- Fibre Channel adapter firmware versions were not showing up as expected in the AHS log.
- Port statistics counters would sometimes not update in the event of Loss of Signal or Loss of Sync
- link downs would occur during specific frame sequences used by the HPE XP8 array after array-side link loss

Please note: Customers with SN1100Q or SN1600Q adapters will need to use a Linux smart component and offline SPP to update to the 2020.09.01 firmware versions for those adapters. See the advisory below for more details.

Customer Advisory: https://support.hpe.com/hpesc/public/docDisplay?docId=emr_na-a00104930en_us

**Prerequisites**

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

The HPE supplied Qlogic driver must be installed prior to this firmware component being identified by SUM for deployment. The OOB driver is available on the Service Pack for ProLiant (SPP) which is available at http://www.hpe.com/servers/spp/download/

**Fixes**

Fixed the following:

- Enhancements have been made to the firmware to prevent and better recover from the unexpected behavior described in Customer Advisory titled: “HPE ProLiant, Synergy and Superdome Flex Host Bus Adapters (HBA) - Certain Fibre Channel HBA Firmware May Cause the Operating System to Halt and Potentially Compromise Filesystem Data Integrity" at the following link:

  https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=a00094722en_us

- Address unexpected behavior when Fibre Channel adapters were simultaneously running traffic to an array which supports 3PAR Persistent Checksum AND another array which is running T10-PI (also known as T10-DIF) or no block checksum technology at all
- Fibre Channel adapter firmware versions were not showing up as expected in the AHS log.
- Port statistics counters would sometimes not update in the event of Loss of Signal or Loss of Sync
- link downs would occur during specific frame sequences used by the HPE XP8 array after array-side link loss\

Please note: Customers with SN1100Q or SN1600Q adapters will need to use a Linux smart component and offline SPP to update to the 2020.09.01 firmware versions for those adapters. See the advisory below for more details.

Customer Advisory: https://support.hpe.com/hpesc/public/docDisplay?docId=emr_na-a00104930en_us

**Enhancements**

Updated the Firmware/BIOS/UEFI packages for 8 Gb, 16 Gb and 32 Gb products.

| Adapter | Speed | MBI | Firmware | UEFI | Boot Bios |
|---|---|---|---|---|---|
| HPE 81Q 8Gb PCIe Fibre Channel Host Bus Adapter | 8Gb | 3.82.00 | 8.08.207 | 7.00 | 3.56 |
| HPE 82Q 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter | 8Gb | 3.82.00 | 8.08.207 | 7.00 | 3.56 |
| HPE 84Q 8Gb Quad Port Fibre Channel Host Bus Adapter | 8Gb | 3.82.00 | 8.08.207 | 7.00 | 3.56 |
| HPE SN1000Q 16GB Dual Port PCIe Fibre Channel Host Bus Adapter | 16Gb | 6.03.00 | 8.08.231 | 7.02 | 3.43 |
| HPE SN1000Q 16GB Single Port PCIe Fibre Channel Host Bus Adapter | 16Gb | 6.03.00 | 8.08.231 | 7.02 | 3.43 |
| HPE SN1610Q 32Gb Dual Port Fibre Channel Host Bus Adapter | 32Gb | 02.03.06 | 09.04.01 | 7.08 | 0.0 |
| HPE SN1610Q 32Gb Single Port Fibre Channel Host Bus Adapter | 32Gb | 02.03.06 | 09.04.01 | 7.08 | 0.0 |

Please note: Customers with SN1100Q or SN1600Q adapters will need to use a Linux smart component and offline SPP to update to the 2020.09.01 firmware versions for those adapters. See the advisory below for more details.

Customer Advisory: https://support.hpe.com/hpesc/public/docDisplay?docId=emr_na-a00104930en_us

**Supported Devices and Features**

This firmware supports the following HPE adapters:

**8Gb Fibre Channel Host Bus Adapter:**

- HPE 81Q 8Gb Single Port PCIe Fibre Channel Host Bus Adapter
- HPE 82Q 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter
- HPE 84Q 8Gb Quad Port Fibre Channel Host Bus Adapter

**16Gb Fibre Channel Host Bus Adapter:**

- HPE SN1000Q 16Gb Dual Port PCIe Fibre Channel Host Bus Adapter
- HPE SN1000Q 16Gb Single Port PCIe Fibre Channel Host Bus Adapter

**32Gb Fibre Channel Host Bus Adapter:**

- HPE SN1610Q 32Gb Dual Port Fibre Channel Host Bus Adapter
- HPE SN1610Q 32Gb Single Port Fibre Channel Host Bus Adapter

---

HPE Firmware Flash for QLogic Fibre Channel Mezzanine Host Bus Adapters for VMware vSphere 7.0
Version: 2020.09.01 **(Recommended)**
Filename: CP042548.compsig; CP042548.zip

**Important Note!**

Release Notes:

HPE QLogic Adapter Release Notes

This Firmware package contains following firmware versions:

| Adapter | Speed | MBI | Firmware | UEFI | Boot Bios |
|---|---|---|---|---|---|
| HPE QMH2572 8Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem | 8Gb | 3.81.05 | 8.08.206 | 7.00 | 3.56 |
| HPE QMH2672 16Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem | 16Gb | 6.02.01 | 8.08.230 | 7.02 | 3.43 |

**Prerequisites**

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

The HPE supplied Qlogic driver must be installed prior to this firmware component being identified by SUM for deployment. The OOB driver is available on the Service Pack for ProLiant (SPP) which is available at http://www.hpe.com/servers/spp/download/

**Enhancements**

Updated the Firmware/BIOS/UEFI packages for 8 Gb and 16 Gb products.

- Gen4 Fibre Channel Host Bus Adapter:
  - Package 3.12.05
  - Firmware 8.08.206
  - UEFI 7.00
  - BIOS 3.56
- Gen5 Fibre Channel Host Bus Adapter:
  - Package 6.02.01
  - Firmware 8.08.230
  - UEFI 7.02
  - BIOS 3.43

**Supported Devices and Features**

This Firmware component supports the following HPE adapters:

**8Gb Fibre Channel Host Bus Adapter:**

- HPE QMH2572 8Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem

**16Gb Fibre Channel Host Bus Adapter:**

- HPE QMH2672 16Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem

---

**Software - Management** Top

HPE Agentless Management Bundle Smart Component on ESXi 7.0 for HPE Gen10/Gen10Plus Servers
Version: 2020.12.01 **(Recommended)**
Filename: cp046012.compsig; cp046012.zip

**Fixes**

- Fix PSOD exception resulting from repeated failed attempts to communicate to iLO
- Fix false NVMe disk temperature alerts
- Fix missing OS, driver and software info from AHS logs
- Fix max and threshold temperature values for SATA disks to prevent fans from running at higher rate
- Fix false SATA disk status change alerts

---

HPE CRU Driver Bundle Smart Component for ESXi 7.0
Version: 2020.04.01 (A) **(Recommended)**
Filename: cp044598.compsig; cp044598.zip

**Enhancements**

Add new supported servers

---

HPE Fiber Channel and Storage Enablement Bundle Smart Component for ESXi 7.0
Version: 2020.09.01 **(Recommended)**
Filename: cp044095.compsig; cp044095.zip

**Enhancements**

Supports VMware ESXi 7.0 and ESXi 7.0 U1

---

HPE iLO Driver Bundle Smart Component for ESXi 7.0
Version: 2020.09.01 **(Recommended)**
Filename: cp043231.compsig; cp043231.zip

**Enhancements**

Supports ESXi 7.0 and ESXi 7.0 U1

---

HPE Smart Storage Administrator (HPE SSA) CLI Smart Component for ESXi 7.0
Version: 2020.09.10 **(Optional)**
Filename: cp044827.compsig; cp044827.zip

**Enhancements**

Added support for HPE Smart Array S100i SR Gen10 Plus SW RAID

---

HPE SMX Provider Bundle Smart Component for ESXi 7.0
Version: 2020.04.01 (A) **(Recommended)**
Filename: cp044591.compsig; cp044591.zip

**Enhancements**

Add new supported servers

---

**Software - System Management** Top

HPE Agentless Management Bundle for ESXi 7.0 for HPE Gen10 and Gen10 Plus Servers
Version: 700.11.6.10 **(Recommended)**
Filename: amsdComponent_700.11.6.10.4-1_17206321.zip

**Fixes**

- Fix PSOD exception resulting from repeated failed attempts to communicate to iLO
- Fix false NVMe disk temperature alerts
- Fix missing OS, driver and software info from AHS logs
- Fix max and threshold temperature values for SATA disks to prevent fans from running at higher rate
- Fix false SATA disk status change alerts

---

HPE Fiber Channel and Storage Enablement Component for ESXi 7.0
Version: 3.6.0 **(Recommended)**
Filename: fc-enablement-component_700.3.6.0.4-1_16239845.zip

**Enhancements**

Supports VMware ESXi 7.0 and ESXi 7.0 U1

---

HPE Smart Storage Administrator (HPE SSA) CLI for VMware 7.0
Version: 4.21.7.0 **(Optional)**
Filename: hpessacli-component_4.21.7.0-7.0.0_15525992.zip

**Enhancements**

Added support for HPE Smart Array S100i SR Gen10 Plus SW RAID

---

HPE SMX Provider Component for ESXi 7.0
Version: 3.16.00 **(Recommended)**
Filename: smxProvider_700.03.16.00__1_.12_14828939_signed_component_1567546.zip

**Enhancements**

Support for VMware ESXi 7.0

---

HPE Utilities Offline Bundle for ESXi 7.0
Version: 10.5.0 **(Recommended)**
Filename: HPE-Utility-Component_10.5.0-63-signed_component-15745486.zip; relnotes.txt

**Important Note!**

Refer to the HPE VMware Utilities User Guide ESXi 7.0 which is located at www.hpe.com/info/vmware/docs.

**Enhancements**

Supports VMware ESXi 7.0

---

Integrated Smart Update Tools for VMware ESXi 7.0
Version: 700.2.7.1 **(Recommended)**
Filename: sutComponent_700.2.7.1.13-0-signed_component-17283720.zip

**Important Note!**

Integrated Smart Update Tools for ESXi 7.0 provides support for firmware and driver updates via iLO Repository

**Fixes**

See the iSUT Release Notes for information about the issues resolved in this release

**Enhancements**

See the iSUT Release Notes for information about the issues resolved in this release

---

Get connected

hpe.com/info/getconnected

Current HPE driver, support, and security alerts delivered directly to your desktop





Trademark acknowledgments, if needed.

Updated August 24 2021

Hewlett Packard Enterprise