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

Gen10 SPP 2024.04.00.00 Release Notes for VMware ESXi 8.0

BIOS - System ROM Top

ROM Flash Firmware Package - HPE Apollo 4200 Gen10/HPE ProLiant XL420 Gen10 (U39) Servers
Version: 3.10_02-22-2024 **(Recommended)**
Filename: U39_3.10_02_22_2024.fwpkg

Important Note!

Important Notes:

This version of the System ROM should be paired with Server Platform Services (SPS) Firmware 04.01.05.002.

Deliverable Name:

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

Release Version:

3.10_02-22-2024

Last Recommended or Critical Revision:

3.10_02-22-2024

Previous Revision:

3.00_10-19-2023

Firmware Dependencies:

None

Enhancements/New Features:

Patch for CVE-2021-38575: The vulnerability allows a remote attacker to execute arbitrary code on the target system.

Patch the primary APIC ID for SMBIOS type 211: Some special CPUs may not have an intra-processor APIC ID == 00h and may cause wrong TControl data.

Patch for CVE-2023-45853: The vulnerability allows a remote attacker to execute arbitrary code on the target system.

The vulnerability exists due to a boundary error in the IScsiHexToBin() function in NetworkPkg/IScsiDxe. A remote attacker with ability to inject data into communication between edk2 and the iSCSI target can execute arbitrary code on the target system.

Prevented a non-standard VPD content from causing the UEFI read function to become write.

Patch for CVE-2022-36763 and CVE-2022-36764: EDK2 is susceptible to a vulnerability in the Tcg2MeasureGptTable() function, allowing a user to trigger a heap buffer overflow via a local network. Successful exploitation of this vulnerability may result in a compromise of confidentiality, integrity, and/or availability.

Added a new event support for IML.

Patch for CVE-2023-45229: EDK2 NetworkPkg Vulnerability

Added an additional retry mechanisms to avoid a BIOS hang from iLO failure.

Corrected Redfish Property value changed from vN_N_N to N.N.N in uri:

/redfish/v1/registrystore/registries/{lang}/biosattributeregistry{Platform}.vN_N_N

there, {lang} = { en, ja, zh }, {platform} = Platform Name e.g. A55, U63 , vN_N_N =

version number defined as Redfish specification

[Example]

uri: /redfish/v1/registrystore/registries/zh/biosattributeregistrya55.v1_1_20

Property of RegistryVersion is changed from v1_1_20 to 1.1.20

Problems Fixed:

Addressed an issue where SBCE and ECC storm records may disappear from AHS.

Addressed an issue where the iSCSI SW IPv6 HDD is not found under OS when the iSCSI IpAddressType is set to Auto.

Addressed an issue where the server may hang due to an IE function error.

Merged the solutions from EDK2 for vulnerabilities:

- Buffer overflow in the DHCPv6 client via a long Server ID option
- Out-of-bounds read when handling a ND Redirect message with truncated options
- Infinite loop when parsing unknown options in the Destination Options header
- Infinite loop when parsing a PadN option in the Destination Options header
- Buffer overflow when processing DNS Servers option in a DHCPv6 Advertise message
- Predictable TCP ISNs
- Use of a Weak PseudoRandom Number Generator

Known Issues:

None

Fixes

Important Notes:

This version of the System ROM should be paired with Server Platform Services (SPS) Firmware 04.01.05.002.

Firmware Dependencies:

None

Problems Fixed:

Addressed an issue where SBCE and ECC storm records may disappear from AHS.

Addressed an issue where the iSCSI SW IPv6 HDD is not found under OS when the iSCSI IpAddressType is set to Auto.

Addressed an issue where the server may hang due to an IE function error.

Merged the solutions from EDK2 for vulnerabilities:

- Buffer overflow in the DHCPv6 client via a long Server ID option
- Out-of-bounds read when handling a ND Redirect message with truncated options
- Infinite loop when parsing unknown options in the Destination Options header
- Infinite loop when parsing a PadN option in the Destination Options header
- Buffer overflow when processing DNS Servers option in a DHCPv6 Advertise message
- Predictable TCP ISNs
- Use of a Weak PseudoRandom Number Generator

Known Issues:

None

Enhancements

Patch for CVE-2021-38575: The vulnerability allows a remote attacker to execute arbitrary code on the target system.

Patch the primary APIC ID for SMBIOS type 211: Some special CPUs may not have an intra-processor APIC ID == 00h and may cause wrong TControl data.

Patch for CVE-2023-45853: The vulnerability allows a remote attacker to execute arbitrary code on the target system.

The vulnerability exists due to a boundary error in the IScsiHexToBin() function in NetworkPkg/IScsiDxe. A remote attacker with ability to inject data into communication between edk2 and the iSCSI target can execute arbitrary code on the target system.

Prevented a non-standard VPD content from causing the UEFI read function to become write.

Patch for CVE-2022-36763 and CVE-2022-36764: EDK2 is susceptible to a vulnerability in the Tcg2MeasureGptTable() function, allowing a user to trigger a heap buffer overflow via a local network. Successful exploitation of this vulnerability may result in a compromise of confidentiality, integrity, and/or availability.

Added a new event support for IML.

Patch for CVE-2023-45229: EDK2 NetworkPkg Vulnerability

Added an additional retry mechanisms to avoid a BIOS hang from iLO failure.

Corrected Redfish Property value changed from vN_N_N to N.N.N in uri:

/redfish/v1/registrystore/registries/{lang}/biosattributeregistry{Platform}.vN_N_N

there, {lang} = { en, ja, zh }, {platform} = Platform Name e.g. A55, U63 , vN_N_N =

version number defined as Redfish specification

[Example]

uri: /redfish/v1/registrystore/registries/zh/biosattributeregistrya55.v1_1_20

Property of RegistryVersion is changed from v1_1_20 to 1.1.20

ROM Flash Firmware Package - HPE Apollo 4510 Gen10/HPE ProLiant XL450 Gen10 (U40) Servers
Version: 3.10_02-22-2024 **(Recommended)**
Filename: U40_3.10_02_22_2024.fwpkg

Important Note!

Important Notes:

This version of the System ROM should be paired with Server Platform Services (SPS) Firmware 04.01.05.002.

Deliverable Name:

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

Release Version:

3.10_02-22-2024

Last Recommended or Critical Revision:

3.10_02-22-2024

Previous Revision:

3.00_10-19-2023

Firmware Dependencies:

None

Enhancements/New Features:

Patch for CVE-2021-38575: The vulnerability allows a remote attacker to execute arbitrary code on the target system.

Patch the primary APIC ID for SMBIOS type 211: Some special CPUs may not have an intra-processor APIC ID == 00h and may cause wrong TControl data.

Patch for CVE-2023-45853: The vulnerability allows a remote attacker to execute arbitrary code on the target system.

The vulnerability exists due to a boundary error in the IScsiHexToBin() function in NetworkPkg/IScsiDxe. A remote attacker with ability to inject data into communication between edk2 and the iSCSI target can execute arbitrary code on the target system.

Prevented a non-standard VPD content from causing the UEFI read function to become write.

Patch for CVE-2022-36763 and CVE-2022-36764: EDK2 is susceptible to a vulnerability in the Tcg2MeasureGptTable() function, allowing a user to trigger a heap buffer overflow via a local network. Successful exploitation of this vulnerability may result in a

compromise of confidentiality, integrity, and/or availability.

Added a new event support for IML.

Patch for CVE-2023-45229: EDK2 NetworkPkg Vulnerability

Added an additional retry mechanisms to avoid a BIOS hang from iLO failure.

Corrected Redfish Property value changed from vN_N_N to N.N.N in uri:

/redfish/v1/registrystore/registries/{lang}/biosattributeregistry{Platform}.vN_N_N

there, {lang} = { en, ja, zh }, {platform} = Platform Name e.g. A55, U63 , vN_N_N =

version number defined as Redfish specification

[Example]

uri: /redfish/v1/registrystore/registries/zh/biosattributeregistrya55.v1_1_20

Property of RegistryVersion is changed from v1_1_20 to 1.1.20

Problems Fixed:

Addressed an issue where SBCE and ECC storm records may disappear from AHS.

Addressed an issue where the iSCSI SW IPv6 HDD is not found under OS when the iSCSI IpAddressType is set to Auto.

Addressed an issue where the server may hang due to an IE function error.

Merged the solutions from EDK2 for vulnerabilities:

- Buffer overflow in the DHCPv6 client via a long Server ID option
- Out-of-bounds read when handling a ND Redirect message with truncated options
- Infinite loop when parsing unknown options in the Destination Options header
- Infinite loop when parsing a PadN option in the Destination Options header
- Buffer overflow when processing DNS Servers option in a DHCPv6 Advertise message
- Predictable TCP ISNs
- Use of a Weak PseudoRandom Number Generator

Known Issues:

None

Fixes

Important Notes:

This version of the System ROM should be paired with Server Platform Services (SPS) Firmware 04.01.05.002.

Firmware Dependencies:

None

Problems Fixed:

Addressed an issue where SBCE and ECC storm records may disappear from AHS.

Addressed an issue where the iSCSI SW IPv6 HDD is not found under OS when the iSCSI IpAddressType is set to Auto.

Addressed an issue where the server may hang due to an IE function error.

Merged the solutions from EDK2 for vulnerabilities:

- Buffer overflow in the DHCPv6 client via a long Server ID option
- Out-of-bounds read when handling a ND Redirect message with truncated options
- Infinite loop when parsing unknown options in the Destination Options header
- Infinite loop when parsing a PadN option in the Destination Options header
- Buffer overflow when processing DNS Servers option in a DHCPv6 Advertise message
- Predictable TCP ISNs
- Use of a Weak PseudoRandom Number Generator

Known Issues:

None

Enhancements

Patch for CVE-2021-38575: The vulnerability allows a remote attacker to execute arbitrary code on the target system.

Patch the primary APIC ID for SMBIOS type 211: Some special CPUs may not have an intra-processor APIC ID == 00h and may cause wrong TControl data.

Patch for CVE-2023-45853: The vulnerability allows a remote attacker to execute arbitrary code on the target system.

The vulnerability exists due to a boundary error in the IScsiHexToBin() function in NetworkPkg/IScsiDxe. A remote attacker with ability to inject data into communication between edk2 and the iSCSI target can execute arbitrary code on the target system.

Prevented a non-standard VPD content from causing the UEFI read function to become write.

Patch for CVE-2022-36763 and CVE-2022-36764: EDK2 is susceptible to a vulnerability in the Tcg2MeasureGptTable() function, allowing a user to trigger a heap buffer overflow via a local network. Successful exploitation of this vulnerability may result in a compromise of confidentiality, integrity, and/or availability.

Added a new event support for IML.

Patch for CVE-2023-45229: EDK2 NetworkPkg Vulnerability

Added an additional retry mechanisms to avoid a BIOS hang from iLO failure.

Corrected Redfish Property value changed from vN_N_N to N.N.N in uri:

/redfish/v1/registrystore/registries/{lang}/biosattributeregistry{Platform}.vN_N_N

there, {lang} = { en, ja, zh }, {platform} = Platform Name e.g. A55, U63 , vN_N_N =

version number defined as Redfish specification

[Example]

uri: /redfish/v1/registrystore/registries/zh/biosattributeregistrya55.v1_1_20

Property of RegistryVersion is changed from v1_1_20 to 1.1.20

ROM Flash Firmware Package - HPE ProLiant DL160 Gen10/DL180 Gen10 (U31) Servers
Version: 3.10_02-22-2024 **(Recommended)**
Filename: U31_3.10_02_22_2024.fwpkg

Important Note!

Important Notes:

This version of the System ROM should be paired with Server Platform Services (SPS) Firmware 04.01.05.002.

Deliverable Name:

HPE ProLiant DL160 Gen10/DL180 Gen10 System ROM - U31

Release Version:

3.10_02-22-2024

Last Recommended or Critical Revision:

3.10_02-22-2024

Previous Revision:

3.00_10-19-2023

Firmware Dependencies:

None

Enhancements/New Features:

Patch for CVE-2021-38575: The vulnerability allows a remote attacker to execute arbitrary code on the target system.

Patch the primary APIC ID for SMBIOS type 211: Some special CPUs may not have an intra-processor APIC ID == 00h and may cause wrong TControl data.

Patch for CVE-2023-45853: The vulnerability allows a remote attacker to execute arbitrary code on the target system.

The vulnerability exists due to a boundary error in the IScsiHexToBin() function in NetworkPkg/IScsiDxe. A remote attacker with ability to inject data into communication between edk2 and the iSCSI target can execute arbitrary code on the target system.

Prevented a non-standard VPD content from causing the UEFI read function to become write.

Patch for CVE-2022-36763 and CVE-2022-36764: EDK2 is susceptible to a vulnerability in the Tcg2MeasureGptTable() function, allowing a user to trigger a heap buffer overflow via a local network. Successful exploitation of this vulnerability may result in a compromise of confidentiality, integrity, and/or availability.

Added a new event support for IML.

Patch for CVE-2023-45229: EDK2 NetworkPkg Vulnerability

Added an additional retry mechanisms to avoid a BIOS hang from iLO failure.

Corrected Redfish Property value changed from vN_N_N to N.N.N in uri:

/redfish/v1/registrystore/registries/{lang}/biosattributeregistry{Platform}.vN_N_N

there, {lang} = { en, ja, zh }, {platform} = Platform Name e.g. A55, U63 , vN_N_N =

version number defined as Redfish specification

[Example]

uri: /redfish/v1/registrystore/registries/zh/biosattributeregistrya55.v1_1_20

Property of RegistryVersion is changed from v1_1_20 to 1.1.20

Problems Fixed:

Addressed an issue where SBCE and ECC storm records may disappear from AHS.

Addressed an issue where the iSCSI SW IPv6 HDD is not found under OS when the iSCSI IpAddressType is set to Auto.

Addressed an issue where the server may hang due to an IE function error.

Merged the solutions from EDK2 for vulnerabilities:

- Buffer overflow in the DHCPv6 client via a long Server ID option

- Out-of-bounds read when handling a ND Redirect message with truncated options

- Infinite loop when parsing unknown options in the Destination Options header

- Infinite loop when parsing a PadN option in the Destination Options header

- Buffer overflow when processing DNS Servers option in a DHCPv6 Advertise message

- Predictable TCP ISNs

- Use of a Weak PseudoRandom Number Generator

Known Issues:

None

Fixes

Important Notes:

This version of the System ROM should be paired with Server Platform Services (SPS) Firmware 04.01.05.002.

Firmware Dependencies:

None

Problems Fixed:

Addressed an issue where SBCE and ECC storm records may disappear from AHS.

Addressed an issue where the iSCSI SW IPv6 HDD is not found under OS when the iSCSI IpAddressType is set to Auto.

Addressed an issue where the server may hang due to an IE function error.

Merged the solutions from EDK2 for vulnerabilities:

- Buffer overflow in the DHCPv6 client via a long Server ID option

- Out-of-bounds read when handling a ND Redirect message with truncated options

- Infinite loop when parsing unknown options in the Destination Options header

- Infinite loop when parsing a PadN option in the Destination Options header

- Buffer overflow when processing DNS Servers option in a DHCPv6 Advertise message

- Predictable TCP ISNs

- Use of a Weak PseudoRandom Number Generator

Known Issues:

None

Enhancements

Patch for CVE-2021-38575: The vulnerability allows a remote attacker to execute arbitrary code on the target system.

Patch the primary APIC ID for SMBIOS type 211: Some special CPUs may not have an intra-processor APIC ID == 00h and may cause wrong TControl data.

Patch for CVE-2023-45853: The vulnerability allows a remote attacker to execute arbitrary code on the target system.

The vulnerability exists due to a boundary error in the IScsiHexToBin() function in NetworkPkg/IScsiDxe. A remote attacker with ability to inject data into communication between edk2 and the iSCSI target can execute arbitrary code on the target system.

Prevented a non-standard VPD content from causing the UEFI read function to become write.

Patch for CVE-2022-36763 and CVE-2022-36764: EDK2 is susceptible to a vulnerability in the Tcg2MeasureGptTable() function, allowing a user to trigger a heap buffer overflow via a local network. Successful exploitation of this vulnerability may result in a compromise of confidentiality, integrity, and/or availability.

Added a new event support for IML.

Patch for CVE-2023-45229: EDK2 NetworkPkg Vulnerability

Added an additional retry mechanisms to avoid a BIOS hang from iLO failure.

Corrected Redfish Property value changed from vN_N_N to N.N.N in uri:

/redfish/v1/registrystore/registries/{lang}/biosattributeregistry{Platform}.vN_N_N

there, {lang} = { en, ja, zh }, {platform} = Platform Name e.g. A55, U63 , vN_N_N =

version number defined as Redfish specification

[Example]

uri: /redfish/v1/registrystore/registries/zh/biosattributeregistrya55.v1_1_20

Property of RegistryVersion is changed from v1_1_20 to 1.1.20

ROM Flash Firmware Package - HPE ProLiant DL20 Gen10 (U43) Servers
Version: 3.00_02-01-2024 **(Recommended)**
Filename: U43_3.00_02_01_2024.fwpkg

Important Note!

Important Notes:

This revision of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2024.1 guidance. This revision of the System ROM includes the mitigation for vulnerabilities documented as CVE-2023-45853 and CVE-2021-38575. This revision of the System ROM includes the revision of the OpenSSL library 1.0.2zi update which provides mitigation for security vulnerabilities documented as CVE-2023-3817. This revision of the System ROM includes the mitigation for NetworkPkg PXE IP stack vulnerabilities documented as CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, and CVE-2023-45237. This version of the System ROM should be paired with Server Platform Services (SPS) Firmware 05.01.04.913.

Deliverable Name:

HPE ProLiant DL20 Gen10 System ROM - U43

Release Version:

3.00_02-01-2024

Last Recommended or Critical Revision:

3.00_02-01-2024

Previous Revision:

2.90_10-19-2023

Firmware Dependencies:

Enhancements/New Features:

Redfish Property value changed from vN_N_N to N.N.N in uri:

/redfish/v1/registrystore/registries/{lang}/biosattributeregistry{Platform}.vN_N_N

there, {lang} = { en, ja, zh }, {platform} = Platform Name e.g. A55, U63 , vN_N_N =

version number defined as Redfish specification

[Example]

uri: /redfish/v1/registrystore/registries/zh/biosattributeregistrya55.v1_1_20

Property of RegistryVersion is changed from v1_1_20 to 1.1.20

Problems Fixed:

This revision of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2024.1 guidance.

This revision of the System ROM includes the mitigation for vulnerabilities documented as CVE-2023-45853 and CVE-2021-38575.

This revision of the System ROM includes the revision of the OpenSSL library 1.0.2zi update which provides mitigation for security vulnerabilities documented as CVE-2023-3817.

This revision of the System ROM includes the mitigation for NetworkPkg PXE IP stack vulnerabilities documented as CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, and CVE-2023-45237.

Addressed an issue where the operating system cannot detect the iSCSI hard drive through IPv6 installation if the iSCSI IpAddressType is set to auto.

Known Issues:

Fixes

Important Notes:

This revision of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2024.1 guidance. This revision of the System ROM includes the mitigation for vulnerabilities documented as CVE-2023-45853 and CVE-2021-38575. This revision of the System ROM includes the revision of the OpenSSL library 1.0.2zi update which provides mitigation for security vulnerabilities documented as CVE-2023-3817. This revision of the System ROM includes the mitigation for NetworkPkg PXE IP stack vulnerabilities documented as CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, and CVE-2023-45237. This version of the System ROM should be paired with Server Platform Services (SPS) Firmware 05.01.04.913.

Firmware Dependencies:

Problems Fixed:

This revision of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2024.1 guidance.

This revision of the System ROM includes the mitigation for vulnerabilities documented as CVE-2023-45853 and CVE-2021-38575.

This revision of the System ROM includes the revision of the OpenSSL library 1.0.2zi update which provides mitigation for security vulnerabilities documented as CVE-2023-3817.

This revision of the System ROM includes the mitigation for NetworkPkg PXE IP stack vulnerabilities documented as CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, and CVE-2023-45237.

Addressed an issue where the operating system cannot detect the iSCSI hard drive through IPv6 installation if the iSCSI IpAddressType is set to auto.

Known Issues:

Enhancements

Redfish Property value changed from vN_N_N to N.N.N in uri:

/redfish/v1/registrystore/registries/{lang}/biosattributeregistry{Platform}.vN_N_N

there, {lang} = { en, ja, zh }, {platform} = Platform Name e.g. A55, U63 , vN_N_N =

version number defined as Redfish specification

[Example]

uri: /redfish/v1/registrystore/registries/zh/biosattributeregistrya55.v1_1_20

Property of RegistryVersion is changed from v1_1_20 to 1.1.20

ROM Flash Firmware Package - HPE Proliant DL20 Gen10 Plus Servers
Version: 2.00_02-01-2024 **(Recommended)**
Filename: U60_2.00_02_01_2024.fwpkg

Important Note!

Important Notes:

This revision of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2024.1 guidance. This revision of the System ROM includes the mitigation for vulnerabilities documented as CVE-2021-38575, CVE-2023-45853, CVE-2022-36763 and CVE-2022-36764. This revision of the System ROM includes the mitigation for NetworkPkg PXE IP stack vulnerabilities documented as CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, and CVE-2023-45237. This version of the System ROM should be paired with Server Platform Services (SPS) Firmware 06.00.03.604 (2.00_12_20_2023).

Deliverable Name:

HPE ProLiant DL20 Gen10 Plus System ROM - U60

Release Version:

2.00_02-01-2024

Last Recommended or Critical Revision:

2.00_02-01-2024

Previous Revision:

1.90_10-19-2023

Firmware Dependencies:

Enhancements/New Features:

Added new Microsoft secure boot keys, KEK2023, Microsoft UEFI CA 2023 and Windows UEFI CA 2023, since the original keys will expire in 2026.

Corrected Redfish Property value changed from vN_N_N to N.N.N in uri:

/redfish/v1/registrystore/registries/{lang}/biosattributeregistry{Platform}.vN_N_N

there, {lang} = { en, ja, zh }, {platform} = Platform Name e.g. A55, U63 , vN_N_N =

version number defined as Redfish specification

[Example]

uri: /redfish/v1/registrystore/registries/zh/biosattributeregistrya55.v1_1_20

Property of RegistryVersion is changed from v1_1_20 to 1.1.20

Added the System Configuration (RBSU) option "Boot Options/UEFI Boot Settings/Filter Non-bootable Drives" and set to "Auto" by default. This setting has the following Redfish property:

/redfish/v1/systems/1/bios/settings/FilterNonbootableDrive

Problems Fixed:

This revision of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2024.1 guidance.

This revision of the System ROM includes the mitigation for vulnerabilities documented as CVE-2021-38575, CVE-2023-45853, CVE-2022-36763 and CVE-2022-36764.

This revision of the System ROM includes the mitigation for NetworkPkg PXE IP stack vulnerabilities documented as CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, and CVE-2023-45237.

Addressed an issue where the operating system cannot detect the iSCSI hard drive through IPv6 installation if the iSCSI IpAddressType is set to auto.

Addressed an issue where DmiAspmCtrl was not set accordingly when setting DMI ASPM to Disabled/L1 Enabled.

Known Issues:

Fixes

Important Notes:

This revision of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2024.1 guidance. This revision of the System ROM includes the mitigation for vulnerabilities documented as CVE-2021-38575, CVE-2023-45853, CVE-2022-36763 and CVE-2022-36764. This revision of the System ROM includes the mitigation for NetworkPkg PXE IP stack vulnerabilities documented as CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, and CVE-2023-45237. This version of the System ROM should be paired with Server Platform Services (SPS) Firmware 06.00.03.604 (2.00_12_20_2023).

Firmware Dependencies:

Problems Fixed:

This revision of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2024.1 guidance.

This revision of the System ROM includes the mitigation for vulnerabilities documented as CVE-2021-38575, CVE-2023-45853, CVE-2022-36763 and CVE-2022-36764.

This revision of the System ROM includes the mitigation for NetworkPkg PXE IP stack vulnerabilities documented as CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, and CVE-2023-45237.

Addressed an issue where the operating system cannot detect the iSCSI hard drive through IPv6 installation if the iSCSI IpAddressType is set to auto.

Addressed an issue where DmiAspmCtrl was not set accordingly when setting DMI ASPM to Disabled/L1 Enabled.

Known Issues:

Enhancements

Added new Microsoft secure boot keys, KEK2023, Microsoft UEFI CA 2023 and Windows UEFI CA 2023, since the original keys will expire in 2026.

Corrected Redfish Property value changed from vN_N_N to N.N.N in uri:

/redfish/v1/registrystore/registries/{lang}/biosattributeregistry{Platform}.vN_N_N

there, {lang} = { en, ja, zh }, {platform} = Platform Name e.g. A55, U63 , vN_N_N =

version number defined as Redfish specification

[Example]

uri: /redfish/v1/registrystore/registries/zh/biosattributeregistrya55.v1_1_20

Property of RegistryVersion is changed from v1_1_20 to 1.1.20

Added the System Configuration (RBSU) option "Boot Options/UEFI Boot Settings/Filter Non-bootable Drives" and set to "Auto" by default. This setting has the following Redfish property:

/redfish/v1/systems/1/bios/settings/FilterNonbootableDrive

ROM Flash Firmware Package - HPE ProLiant DL325 Gen10 (A41) Servers
Version: 3.00_01-26-2024 **(Recommended)**
Filename: A41_3.00_01_26_2024.fwpkg

Important Note!

Important Notes:

This version of the System ROM contains updates aligned with vulnerability fixes in EDK2 NetworkPkg IP stack implementation that is described in the address https://github.com/tianocore/edk2/security/advisories/GHSA-hc6x-cw6p-gj7h.

Deliverable Name:

HPE ProLiant DL325 Gen10 System ROM - A41

Release Version:

3.00_01-26-2024

Last Recommended or Critical Revision:

3.00_01-26-2024

Previous Revision:

2.90_10-19-2023

Firmware Dependencies:

None

Enhancements/New Features:

None

Problems Fixed:

This revision of the System ROM includes the mitigation for NetworkPkg PXE IP stack vulnerabilities documented as CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, and CVE-2023-45237.

Known Issues:

None

Fixes

Important Notes:

This version of the System ROM contains updates aligned with vulnerability fixes in EDK2 NetworkPkg IP stack implementation that is described in the address https://github.com/tianocore/edk2/security/advisories/GHSA-hc6x-cw6p-gj7h.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the mitigation for NetworkPkg PXE IP stack vulnerabilities documented as CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, and CVE-2023-45237.

Known Issues:

None

ROM Flash Firmware Package - HPE ProLiant DL360 Gen10 (U32) Servers
Version: 3.10_02-22-2024 **(Recommended)**
Filename: U32_3.10_02_22_2024.fwpkg

Important Note!

Important Notes:

This version of the System ROM should be paired with Server Platform Services (SPS) Firmware 04.01.05.002.

Deliverable Name:

HPE ProLiant DL360 Gen10 System ROM - U32

Release Version:

3.10_02-22-2024

Last Recommended or Critical Revision:

3.10_02-22-2024

Previous Revision:

3.00_10-19-2023

Firmware Dependencies:

None

Enhancements/New Features:

Patch for CVE-2021-38575: The vulnerability allows a remote attacker to execute arbitrary code on the target system.

Patch the primary APIC ID for SMBIOS type 211: Some special CPUs may not have an intra-processor APIC ID == 00h and may cause wrong TControl data.

Patch for CVE-2023-45853: The vulnerability allows a remote attacker to execute arbitrary code on the target system.

The vulnerability exists due to a boundary error in the IScsiHexToBin() function in NetworkPkg/IScsiDxe. A remote attacker with ability to inject data into communication between edk2 and the iSCSI target can execute arbitrary code on the target system.

Prevented a non-standard VPD content from causing the UEFI read function to become write.

Patch for CVE-2022-36763 and CVE-2022-36764: EDK2 is susceptible to a vulnerability in the Tcg2MeasureGptTable() function, allowing a user to trigger a heap buffer overflow via a local network. Successful exploitation of this vulnerability may result in a compromise of confidentiality, integrity, and/or availability.

Added a new event support for IML.

Patch for CVE-2023-45229: EDK2 NetworkPkg Vulnerability

Added an additional retry mechanisms to avoid a BIOS hang from iLO failure.

Corrected Redfish Property value changed from vN_N_N to N.N.N in uri:

/redfish/v1/registrystore/registries/{lang}/biosattributeregistry{Platform}.vN_N_N

there, {lang} = { en, ja, zh }, {platform} = Platform Name e.g. A55, U63 , vN_N_N =

version number defined as Redfish specification

[Example]

uri: /redfish/v1/registrystore/registries/zh/biosattributeregistrya55.v1_1_20

Property of RegistryVersion is changed from v1_1_20 to 1.1.20

Problems Fixed:

Addressed an issue where SBCE and ECC storm records may disappear from AHS.

Addressed an issue where the iSCSI SW IPv6 HDD is not found under OS when the iSCSI IpAddressType is set to Auto.

Addressed an issue where the server may hang due to an IE function error.

Merged the solutions from EDK2 for vulnerabilities:

- Buffer overflow in the DHCPv6 client via a long Server ID option

- Out-of-bounds read when handling a ND Redirect message with truncated options

- Infinite loop when parsing unknown options in the Destination Options header

- Infinite loop when parsing a PadN option in the Destination Options header

- Buffer overflow when processing DNS Servers option in a DHCPv6 Advertise message

- Predictable TCP ISNs

- Use of a Weak PseudoRandom Number Generator

Known Issues:

None

Fixes

Important Notes:

This version of the System ROM should be paired with Server Platform Services (SPS) Firmware 04.01.05.002.

Firmware Dependencies:

None

Problems Fixed:

Addressed an issue where SBCE and ECC storm records may disappear from AHS.

Addressed an issue where the iSCSI SW IPv6 HDD is not found under OS when the iSCSI IpAddressType is set to Auto.

Addressed an issue where the server may hang due to an IE function error.

Merged the solutions from EDK2 for vulnerabilities:

- Buffer overflow in the DHCPv6 client via a long Server ID option

- Out-of-bounds read when handling a ND Redirect message with truncated options

- Infinite loop when parsing unknown options in the Destination Options header

- Infinite loop when parsing a PadN option in the Destination Options header

- Buffer overflow when processing DNS Servers option in a DHCPv6 Advertise message

- Predictable TCP ISNs

- Use of a Weak PseudoRandom Number Generator

Known Issues:

None

Enhancements

Patch for CVE-2021-38575: The vulnerability allows a remote attacker to execute arbitrary code on the target system.

Patch the primary APIC ID for SMBIOS type 211: Some special CPUs may not have an intra-processor APIC ID == 00h and may cause wrong TControl data.

Patch for CVE-2023-45853: The vulnerability allows a remote attacker to execute arbitrary code on the target system.

The vulnerability exists due to a boundary error in the IScsiHexToBin() function in NetworkPkg/IScsiDxe. A remote attacker with ability to inject data into communication between edk2 and the iSCSI target can execute arbitrary code on the target system.

Prevented a non-standard VPD content from causing the UEFI read function to become write.

Patch for CVE-2022-36763 and CVE-2022-36764: EDK2 is susceptible to a vulnerability in the Tcg2MeasureGptTable() function, allowing a user to trigger a heap buffer overflow via a local network. Successful exploitation of this vulnerability may result in a compromise of confidentiality, integrity, and/or availability.

Added a new event support for IML.

Patch for CVE-2023-45229: EDK2 NetworkPkg Vulnerability

Added an additional retry mechanisms to avoid a BIOS hang from iLO failure.

Corrected Redfish Property value changed from vN_N_N to N.N.N in uri:

/redfish/v1/registrystore/registries/{lang}/biosattributeregistry{Platform}.vN_N_N

there, {lang} = { en, ja, zh }, {platform} = Platform Name e.g. A55, U63 , vN_N_N =

version number defined as Redfish specification

[Example]

uri: /redfish/v1/registrystore/registries/zh/biosattributeregistrya55.v1_1_20

Property of RegistryVersion is changed from v1_1_20 to 1.1.20

ROM Flash Firmware Package - HPE ProLiant DL380 Gen10 (U30) Servers
Version: 3.10_02-22-2024 **(Recommended)**
Filename: U30_3.10_02_22_2024.fwpkg

Important Note!

Important Notes:

This version of the System ROM should be paired with Server Platform Services (SPS) Firmware 04.01.05.002.

Deliverable Name:

HPE ProLiant DL380 Gen10 System ROM - U30

Release Version:

3.10_02-22-2024

Last Recommended or Critical Revision:

3.10_02-22-2024

Previous Revision:

3.00_10-19-2023

Firmware Dependencies:

None

Enhancements/New Features:

Patch for CVE-2021-38575: The vulnerability allows a remote attacker to execute arbitrary code on the target system.

Patch the primary APIC ID for SMBIOS type 211: Some special CPUs may not have an intra-processor APIC ID == 00h and may cause wrong TControl data.

Patch for CVE-2023-45853: The vulnerability allows a remote attacker to execute arbitrary code on the target system.

The vulnerability exists due to a boundary error in the IScsiHexToBin() function in NetworkPkg/IScsiDxe. A remote attacker with ability to inject data into communication between edk2 and the iSCSI target can execute arbitrary code on the target system.

Prevented a non-standard VPD content from causing the UEFI read function to become write.

Patch for CVE-2022-36763 and CVE-2022-36764: EDK2 is susceptible to a vulnerability in the Tcg2MeasureGptTable() function, allowing a user to trigger a heap buffer overflow via a local network. Successful exploitation of this vulnerability may result in a compromise of confidentiality, integrity, and/or availability.

Added a new event support for IML.

Patch for CVE-2023-45229: EDK2 NetworkPkg Vulnerability

Added an additional retry mechanisms to avoid a BIOS hang from iLO failure.

Corrected Redfish Property value changed from vN_N_N to N.N.N in uri:

/redfish/v1/registrystore/registries/{lang}/biosattributeregistry{Platform}.vN_N_N

there, {lang} = { en, ja, zh }, {platform} = Platform Name e.g. A55, U63 , vN_N_N =

version number defined as Redfish specification

[Example]

uri: /redfish/v1/registrystore/registries/zh/biosattributeregistrya55.v1_1_20

Property of RegistryVersion is changed from v1_1_20 to 1.1.20

Problems Fixed:

Addressed an issue where SBCE and ECC storm records may disappear from AHS.

Addressed an issue where the iSCSI SW IPv6 HDD is not found under OS when the iSCSI IpAddressType is set to Auto.

Addressed an issue where the server may hang due to an IE function error.

Merged the solutions from EDK2 for vulnerabilities:

- Buffer overflow in the DHCPv6 client via a long Server ID option

- Out-of-bounds read when handling a ND Redirect message with truncated options

- Infinite loop when parsing unknown options in the Destination Options header

- Infinite loop when parsing a PadN option in the Destination Options header

- Buffer overflow when processing DNS Servers option in a DHCPv6 Advertise message

- Predictable TCP ISNs

- Use of a Weak PseudoRandom Number Generator

Known Issues:

None

Fixes

Important Notes:

This version of the System ROM should be paired with Server Platform Services (SPS) Firmware 04.01.05.002.

Firmware Dependencies:

None

Problems Fixed:

Addressed an issue where SBCE and ECC storm records may disappear from AHS.

Addressed an issue where the iSCSI SW IPv6 HDD is not found under OS when the iSCSI IpAddressType is set to Auto.

Addressed an issue where the server may hang due to an IE function error.

Merged the solutions from EDK2 for vulnerabilities:

- Buffer overflow in the DHCPv6 client via a long Server ID option

- Out-of-bounds read when handling a ND Redirect message with truncated options

- Infinite loop when parsing unknown options in the Destination Options header

- Infinite loop when parsing a PadN option in the Destination Options header

- Buffer overflow when processing DNS Servers option in a DHCPv6 Advertise message

- Predictable TCP ISNs

- Use of a Weak PseudoRandom Number Generator

Known Issues:

None

Enhancements

Patch for CVE-2021-38575: The vulnerability allows a remote attacker to execute arbitrary code on the target system.

Patch the primary APIC ID for SMBIOS type 211: Some special CPUs may not have an intra-processor APIC ID == 00h and may cause wrong TControl data.

Patch for CVE-2023-45853: The vulnerability allows a remote attacker to execute arbitrary code on the target system.

The vulnerability exists due to a boundary error in the IScsiHexToBin() function in NetworkPkg/IScsiDxe. A remote attacker with ability to inject data into communication between edk2 and the iSCSI target can execute arbitrary code on the target system.

Prevented a non-standard VPD content from causing the UEFI read function to become write.

Patch for CVE-2022-36763 and CVE-2022-36764: EDK2 is susceptible to a vulnerability in the Tcg2MeasureGptTable() function, allowing a user to trigger a heap buffer overflow via a local network. Successful exploitation of this vulnerability may result in a compromise of confidentiality, integrity, and/or availability.

Added a new event support for IML.

Patch for CVE-2023-45229: EDK2 NetworkPkg Vulnerability

Added an additional retry mechanisms to avoid a BIOS hang from iLO failure.

Corrected Redfish Property value changed from vN_N_N to N.N.N in uri:

/redfish/v1/registrystore/registries/{lang}/biosattributeregistry{Platform}.vN_N_N

there, {lang} = { en, ja, zh }, {platform} = Platform Name e.g. A55, U63 , vN_N_N =

version number defined as Redfish specification

[Example]

uri: /redfish/v1/registrystore/registries/zh/biosattributeregistrya55.v1_1_20

Property of RegistryVersion is changed from v1_1_20 to 1.1.20

ROM Flash Firmware Package - HPE ProLiant DL385 Gen10 (A40) Servers
Version: 3.00_01-26-2024 **(Recommended)**
Filename: A40_3.00_01_26_2024.fwpkg

Important Note!

Important Notes:

This version of the System ROM contains updates aligned with vulnerability fixes in EDK2 NetworkPkg IP stack implementation that is described in the address https://github.com/tianocore/edk2/security/advisories/GHSA-hc6x-cw6p-gj7h.

Deliverable Name:

HPE DL385Gen10 System ROM - A40

Release Version:

3.00_01-26-2024

Last Recommended or Critical Revision:

3.00_01-26-2024

Previous Revision:

2.90_10-19-2023

Firmware Dependencies:

None

Enhancements/New Features:

None

Problems Fixed:

This revision of the System ROM includes the mitigation for NetworkPkg PXE IP stack vulnerabilities documented as CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, and CVE-2023-45237.

Known Issues:

None

Fixes

Important Notes:

This version of the System ROM contains updates aligned with vulnerability fixes in EDK2 NetworkPkg IP stack implementation that is described in the address https://github.com/tianocore/edk2/security/advisories/GHSA-hc6x-cw6p-gj7h.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the mitigation for NetworkPkg PXE IP stack vulnerabilities documented as CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, and CVE-2023-45237.

Known Issues:

None

ROM Flash Firmware Package - HPE ProLiant DL560 Gen10/DL580 Gen10 (U34) Servers
Version: 3.10_02-22-2024 **(Recommended)**
Filename: U34_3.10_02_22_2024.fwpkg

Important Note!

Important Notes:

This version of the System ROM should be paired with Server Platform Services (SPS) Firmware 04.01.05.002.

Deliverable Name:

HPE ProLiant DL560 Gen10/DL580 Gen10 System ROM - U34

Release Version:

3.10_02-22-2024

Last Recommended or Critical Revision:

3.10_02-22-2024

Previous Revision:

3.00_10-19-2023

Firmware Dependencies:

None

Enhancements/New Features:

Patch for CVE-2021-38575: The vulnerability allows a remote attacker to execute arbitrary code on the target system.

Patch the primary APIC ID for SMBIOS type 211: Some special CPUs may not have an intra-processor APIC ID == 00h and may cause wrong TControl data.

Patch for CVE-2023-45853: The vulnerability allows a remote attacker to execute arbitrary code on the target system.

The vulnerability exists due to a boundary error in the IScsiHexToBin() function in NetworkPkg/IScsiDxe. A remote attacker with ability to inject data into communication between edk2 and the iSCSI target can execute arbitrary code on the target system.

Prevented a non-standard VPD content from causing the UEFI read function to become write.

Patch for CVE-2022-36763 and CVE-2022-36764: EDK2 is susceptible to a vulnerability in the Tcg2MeasureGptTable() function, allowing a user to trigger a heap buffer overflow via a local network. Successful exploitation of this vulnerability may result in a compromise of confidentiality, integrity, and/or availability.

Added a new event support for IML.

Patch for CVE-2023-45229: EDK2 NetworkPkg Vulnerability

Added an additional retry mechanisms to avoid a BIOS hang from iLO failure.

Corrected Redfish Property value changed from vN_N_N to N.N.N in uri:

/redfish/v1/registrystore/registries/{lang}/biosattributeregistry{Platform}.vN_N_N

there, {lang} = { en, ja, zh }, {platform} = Platform Name e.g. A55, U63 , vN_N_N =

version number defined as Redfish specification

[Example]

uri: /redfish/v1/registrystore/registries/zh/biosattributeregistrya55.v1_1_20

Property of RegistryVersion is changed from v1_1_20 to 1.1.20

Problems Fixed:

Addressed an issue where SBCE and ECC storm records may disappear from AHS.

Addressed an issue where the iSCSI SW IPv6 HDD is not found under OS when the iSCSI IpAddressType is set to Auto.

Addressed an issue where the server may hang due to an IE function error.

Merged the solutions from EDK2 for vulnerabilities:

- Buffer overflow in the DHCPv6 client via a long Server ID option

- Out-of-bounds read when handling a ND Redirect message with truncated options

- Infinite loop when parsing unknown options in the Destination Options header

- Infinite loop when parsing a PadN option in the Destination Options header

- Buffer overflow when processing DNS Servers option in a DHCPv6 Advertise message

- Predictable TCP ISNs

- Use of a Weak PseudoRandom Number Generator

Known Issues:

None

Fixes

Important Notes:

This version of the System ROM should be paired with Server Platform Services (SPS) Firmware 04.01.05.002.

Firmware Dependencies:

None

Problems Fixed:

Addressed an issue where SBCE and ECC storm records may disappear from AHS.

Addressed an issue where the iSCSI SW IPv6 HDD is not found under OS when the iSCSI IpAddressType is set to Auto.

Addressed an issue where the server may hang due to an IE function error.

Merged the solutions from EDK2 for vulnerabilities:

- Buffer overflow in the DHCPv6 client via a long Server ID option

- Out-of-bounds read when handling a ND Redirect message with truncated options

- Infinite loop when parsing unknown options in the Destination Options header

- Infinite loop when parsing a PadN option in the Destination Options header

- Buffer overflow when processing DNS Servers option in a DHCPv6 Advertise message

- Predictable TCP ISNs

- Use of a Weak PseudoRandom Number Generator

Known Issues:

None

Enhancements

Patch for CVE-2021-38575: The vulnerability allows a remote attacker to execute arbitrary code on the target system.

Patch the primary APIC ID for SMBIOS type 211: Some special CPUs may not have an intra-processor APIC ID == 00h and may cause wrong TControl data.

Patch for CVE-2023-45853: The vulnerability allows a remote attacker to execute arbitrary code on the target system.

The vulnerability exists due to a boundary error in the IScsiHexToBin() function in NetworkPkg/IScsiDxe. A remote attacker with ability to inject data into communication between edk2 and the iSCSI target can execute arbitrary code on the target system.

Prevented a non-standard VPD content from causing the UEFI read function to become write.

Patch for CVE-2022-36763 and CVE-2022-36764: EDK2 is susceptible to a vulnerability in the Tcg2MeasureGptTable() function, allowing a user to trigger a heap buffer overflow via a local network. Successful exploitation of this vulnerability may result in a compromise of confidentiality, integrity, and/or availability.

Added a new event support for IML.

Patch for CVE-2023-45229: EDK2 NetworkPkg Vulnerability

Added an additional retry mechanisms to avoid a BIOS hang from iLO failure.

Corrected Redfish Property value changed from vN_N_N to N.N.N in uri:

/redfish/v1/registrystore/registries/{lang}/biosattributeregistry{Platform}.vN_N_N

there, {lang} = { en, ja, zh }, {platform} = Platform Name e.g. A55, U63 , vN_N_N =

version number defined as Redfish specification

[Example]

uri: /redfish/v1/registrystore/registries/zh/biosattributeregistrya55.v1_1_20

Property of RegistryVersion is changed from v1_1_20 to 1.1.20

ROM Flash Firmware Package - HPE ProLiant MicroServer Gen10 Plus v2 (U64) Servers
Version: 2.00_02-01-2024 **(Recommended)**
Filename: U64_2.00_02_01_2024.fwpkg

Important Note!

Important Notes:

This revision of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2024.1 guidance. This revision of the System ROM includes the mitigation for vulnerabilities documented as CVE-2021-38575, CVE-2023-45853, CVE-2022-36763 and CVE-2022-36764. This revision of the System ROM includes the mitigation for NetworkPkg PXE IP stack vulnerabilities documented as CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, and CVE-2023-45237. This version of the System ROM should be paired with Server Platform Services (SPS) Firmware 06.00.03.604 (2.00_12_20_2023).

Deliverable Name:

HPE ProLiant MicroServer Gen10 Plus v2 System ROM - U64

Release Version:

2.00_02-01-2024

Last Recommended or Critical Revision:

2.00_02-01-2024

Previous Revision:

1.90_10-19-2023

Firmware Dependencies:

Enhancements/New Features:

Added new Microsoft secure boot keys, KEK2023, Microsoft UEFI CA 2023 and Windows UEFI CA 2023, since the original keys will expire in 2026.

Corrected Redfish Property value changed from vN_N_N to N.N.N in uri:

/redfish/v1/registrystore/registries/{lang}/biosattributeregistry{Platform}.vN_N_N

there, {lang} = { en, ja, zh }, {platform} = Platform Name e.g. A55, U63 , vN_N_N =

version number defined as Redfish specification

[Example]

uri: /redfish/v1/registrystore/registries/zh/biosattributeregistrya55.v1_1_20

Property of RegistryVersion is changed from v1_1_20 to 1.1.20

Added the System Configuration (RBSU) option "Boot Options/UEFI Boot Settings/Filter Non-bootable Drives" and set to "Auto" by default. This setting has the following Redfish property:

/redfish/v1/systems/1/bios/settings/FilterNonbootableDrive

Problems Fixed:

This revision of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2024.1 guidance.

This revision of the System ROM includes the mitigation for vulnerabilities documented as CVE-2021-38575, CVE-2023-45853, CVE-2022-36763 and CVE-2022-36764.

This revision of the System ROM includes the mitigation for NetworkPkg PXE IP stack vulnerabilities documented as CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, and CVE-2023-45237.

Addressed an issue where the operating system cannot detect the iSCSI hard drive through IPv6 installation if the iSCSI IpAddressType is set to auto.

Addressed an issue where DmiAspmCtrl was not set accordingly when setting DMI ASPM to Disabled/L1 Enabled.

Known Issues:

Fixes

Important Notes:

This revision of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2024.1 guidance. This revision of the System ROM includes the mitigation for vulnerabilities documented as CVE-2021-38575, CVE-2023-45853, CVE-2022-36763 and CVE-2022-36764. This revision of the System ROM includes the mitigation for NetworkPkg PXE IP stack vulnerabilities documented as CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, and CVE-2023-45237. This version of the System ROM should be paired with Server Platform Services (SPS) Firmware 06.00.03.604 (2.00_12_20_2023).

Firmware Dependencies:

Problems Fixed:

This revision of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2024.1 guidance.

This revision of the System ROM includes the mitigation for vulnerabilities documented as CVE-2021-38575, CVE-2023-45853, CVE-2022-36763 and CVE-2022-36764.

This revision of the System ROM includes the mitigation for NetworkPkg PXE IP stack vulnerabilities documented as CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, and CVE-2023-45237.

Addressed an issue where the operating system cannot detect the iSCSI hard drive through IPv6 installation if the iSCSI IpAddressType is set to auto.

Addressed an issue where DmiAspmCtrl was not set accordingly when setting DMI ASPM to Disabled/L1 Enabled.

Known Issues:

Enhancements

Added new Microsoft secure boot keys, KEK2023, Microsoft UEFI CA 2023 and Windows UEFI CA 2023, since the original keys will expire in 2026.

Corrected Redfish Property value changed from vN_N_N to N.N.N in uri:

/redfish/v1/registrystore/registries/{lang}/biosattributeregistry{Platform}.vN_N_N

there, {lang} = { en, ja, zh }, {platform} = Platform Name e.g. A55, U63 , vN_N_N =

version number defined as Redfish specification

[Example]

uri: /redfish/v1/registrystore/registries/zh/biosattributeregistrya55.v1_1_20

Property of RegistryVersion is changed from v1_1_20 to 1.1.20

Added the System Configuration (RBSU) option "Boot Options/UEFI Boot Settings/Filter Non-bootable Drives" and set to "Auto" by default. This setting has the following Redfish property:

/redfish/v1/systems/1/bios/settings/FilterNonbootableDrive

ROM Flash Firmware Package - HPE ProLiant ML110 Gen10 (U33) Servers
Version: 3.10_02-22-2024 **(Recommended)**
Filename: U33_3.10_02_22_2024.fwpkg

Important Note!

Important Notes:

This version of the System ROM should be paired with Server Platform Services (SPS) Firmware 04.01.05.002.

Deliverable Name:

HPE ProLiant ML110 Gen10 System ROM - U33

Release Version:

3.10_02-22-2024

Last Recommended or Critical Revision:

3.10_02-22-2024

Previous Revision:

3.00_10-19-2023

Firmware Dependencies:

None

Enhancements/New Features:

Patch for CVE-2021-38575: The vulnerability allows a remote attacker to execute arbitrary code on the target system.

Patch the primary APIC ID for SMBIOS type 211: Some special CPUs may not have an intra-processor APIC ID == 00h and may cause wrong TControl data.

Patch for CVE-2023-45853: The vulnerability allows a remote attacker to execute arbitrary code on the target system.

The vulnerability exists due to a boundary error in the IScsiHexToBin() function in NetworkPkg/IScsiDxe. A remote attacker with ability to inject data into communication between edk2 and the iSCSI target can execute arbitrary code on the target system.

Prevented a non-standard VPD content from causing the UEFI read function to become write.

Patch for CVE-2022-36763 and CVE-2022-36764: EDK2 is susceptible to a vulnerability in the Tcg2MeasureGptTable() function, allowing a user to trigger a heap buffer overflow via a local network. Successful exploitation of this vulnerability may result in a compromise of confidentiality, integrity, and/or availability.

Added a new event support for IML.

Patch for CVE-2023-45229: EDK2 NetworkPkg Vulnerability

Added an additional retry mechanisms to avoid a BIOS hang from iLO failure.

Corrected Redfish Property value changed from vN_N_N to N.N.N in uri:

/redfish/v1/registrystore/registries/{lang}/biosattributeregistry{Platform}.vN_N_N

there, {lang} = { en, ja, zh }, {platform} = Platform Name e.g. A55, U63 , vN_N_N =

version number defined as Redfish specification

[Example]

uri: /redfish/v1/registrystore/registries/zh/biosattributeregistrya55.v1_1_20

Property of RegistryVersion is changed from v1_1_20 to 1.1.20

Problems Fixed:

Addressed an issue where SBCE and ECC storm records may disappear from AHS.

Addressed an issue where the iSCSI SW IPv6 HDD is not found under OS when the iSCSI IpAddressType is set to Auto.

Addressed an issue where the server may hang due to an IE function error.

Merged the solutions from EDK2 for vulnerabilities:

- Buffer overflow in the DHCPv6 client via a long Server ID option
- Out-of-bounds read when handling a ND Redirect message with truncated options
- Infinite loop when parsing unknown options in the Destination Options header
- Infinite loop when parsing a PadN option in the Destination Options header
- Buffer overflow when processing DNS Servers option in a DHCPv6 Advertise message
- Predictable TCP ISNs
- Use of a Weak PseudoRandom Number Generator

Known Issues:

None

Fixes

Important Notes:

This version of the System ROM should be paired with Server Platform Services (SPS) Firmware 04.01.05.002.

Firmware Dependencies:

None

Problems Fixed:

Addressed an issue where SBCE and ECC storm records may disappear from AHS.

Addressed an issue where the iSCSI SW IPv6 HDD is not found under OS when the iSCSI IpAddressType is set to Auto.

Addressed an issue where the server may hang due to an IE function error.

Merged the solutions from EDK2 for vulnerabilities:

- Buffer overflow in the DHCPv6 client via a long Server ID option
- Out-of-bounds read when handling a ND Redirect message with truncated options
- Infinite loop when parsing unknown options in the Destination Options header
- Infinite loop when parsing a PadN option in the Destination Options header
- Buffer overflow when processing DNS Servers option in a DHCPv6 Advertise message
- Predictable TCP ISNs
- Use of a Weak PseudoRandom Number Generator

Known Issues:

None

Enhancements

Patch for CVE-2021-38575: The vulnerability allows a remote attacker to execute arbitrary code on the target system.

Patch the primary APIC ID for SMBIOS type 211: Some special CPUs may not have an intra-processor APIC ID == 00h and may cause wrong TControl data.

Patch for CVE-2023-45853: The vulnerability allows a remote attacker to execute arbitrary code on the target system.

The vulnerability exists due to a boundary error in the IScsiHexToBin() function in NetworkPkg/IScsiDxe. A remote attacker with ability to inject data into communication between edk2 and the iSCSI target can execute arbitrary code on the target system.

Prevented a non-standard VPD content from causing the UEFI read function to become write.

Patch for CVE-2022-36763 and CVE-2022-36764: EDK2 is susceptible to a vulnerability in the Tcg2MeasureGptTable() function, allowing a user to trigger a heap buffer overflow via a local network. Successful exploitation of this vulnerability may result in a compromise of confidentiality, integrity, and/or availability.

Added a new event support for IML.

Patch for CVE-2023-45229: EDK2 NetworkPkg Vulnerability

Added an additional retry mechanisms to avoid a BIOS hang from iLO failure.

Corrected Redfish Property value changed from vN_N_N to N.N.N in uri:

/redfish/v1/registrystore/registries/{lang}/biosattributeregistry{Platform}.vN_N_N

there, {lang} = { en, ja, zh }, {platform} = Platform Name e.g. A55, U63 , vN_N_N =

version number defined as Redfish specification

[Example]

uri: /redfish/v1/registrystore/registries/zh/biosattributeregistrya55.v1_1_20

Property of RegistryVersion is changed from v1_1_20 to 1.1.20

ROM Flash Firmware Package - HPE ProLiant ML30 Gen10 (U44) Servers
Version: 3.00_02-01-2024 **(Recommended)**
Filename: U44_3.00_02_01_2024.fwpkg

Important Note!

Important Notes:

This revision of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2024.1 guidance. This revision of the System ROM includes the mitigation for vulnerabilities documented as CVE-2023-45853 and CVE-2021-38575. This revision of the System ROM includes the revision of the OpenSSL library 1.0.2zi update which provides mitigation for security vulnerabilities documented as CVE-2023-3817. This revision of the System ROM includes the mitigation for NetworkPkg PXE IP stack vulnerabilities documented as CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, and CVE-2023-45237. This version of the System ROM should be paired with Server Platform Services (SPS) Firmware 05.01.04.913.

Deliverable Name:

HPE ProLiant ML30 Gen10 System ROM - U44

Release Version:

3.00_02-01-2024

Last Recommended or Critical Revision:

3.00_02-01-2024

Previous Revision:

2.90_10-19-2023

Firmware Dependencies:

Enhancements/New Features:

Redfish Property value changed from vN_N_N to N.N.N in uri:

/redfish/v1/registrystore/registries/{lang}/biosattributeregistry{Platform}.vN_N_N

there, {lang} = { en, ja, zh }, {platform} = Platform Name e.g. A55, U63 , vN_N_N =

version number defined as Redfish specification

[Example]

uri: /redfish/v1/registrystore/registries/zh/biosattributeregistrya55.v1_1_20

Property of RegistryVersion is changed from v1_1_20 to 1.1.20

Problems Fixed:

This revision of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2024.1 guidance.

This revision of the System ROM includes the mitigation for vulnerabilities documented as CVE-2023-45853 and CVE-2021-38575.

This revision of the System ROM includes the revision of the OpenSSL library 1.0.2zi update which provides mitigation for security vulnerabilities documented as CVE-2023-3817.

This revision of the System ROM includes the mitigation for NetworkPkg PXE IP stack vulnerabilities documented as CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, and CVE-2023-45237.

Addressed an issue where the operating system cannot detect the iSCSI hard drive through IPv6 installation if the iSCSI IpAddressType is set to auto.

Known Issues:

Fixes

Important Notes:

This revision of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2024.1 guidance. This revision of the System ROM includes the mitigation for vulnerabilities documented as CVE-2023-45853 and CVE-2021-38575. This revision of the System ROM includes the revision of the OpenSSL library 1.0.2zi update which provides mitigation for security vulnerabilities documented as CVE-2023-3817. This revision of the System ROM includes the mitigation for NetworkPkg PXE IP stack vulnerabilities documented as CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, and CVE-2023-45237. This version of the System ROM should be paired with Server Platform Services (SPS) Firmware 05.01.04.913.

Firmware Dependencies:

Problems Fixed:

This revision of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2024.1 guidance.

This revision of the System ROM includes the mitigation for vulnerabilities documented as CVE-2023-45853 and CVE-2021-38575.

This revision of the System ROM includes the revision of the OpenSSL library 1.0.2zi update which provides mitigation for security vulnerabilities documented as CVE-2023-3817.

This revision of the System ROM includes the mitigation for NetworkPkg PXE IP stack vulnerabilities documented as CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, and CVE-2023-45237.

Addressed an issue where the operating system cannot detect the iSCSI hard drive through IPv6 installation if the iSCSI IpAddressType is set to auto.

Known Issues:

Enhancements

Redfish Property value changed from vN_N_N to N.N.N in uri:

/redfish/v1/registrystore/registries/{lang}/biosattributeregistry{Platform}.vN_N_N

there, {lang} = { en, ja, zh }, {platform} = Platform Name e.g. A55, U63 , vN_N_N =

version number defined as Redfish specification

[Example]

uri: /redfish/v1/registrystore/registries/zh/biosattributeregistrya55.v1_1_20

Property of RegistryVersion is changed from v1_1_20 to 1.1.20

ROM Flash Firmware Package - HPE ProLiant ML30 Gen10 Plus Servers
Version: 2.00_02-01-2024 **(Recommended)**
Filename: U61_2.00_02_01_2024.fwpkg

Important Note!

Important Notes:

This revision of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2024.1 guidance. This revision of the System ROM includes the mitigation for vulnerabilities documented as CVE-2021-38575, CVE-2023-45853, CVE-2022-36763 and CVE-2022-36764. This revision of the System ROM includes the mitigation for NetworkPkg PXE IP stack vulnerabilities documented as CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, and CVE-2023-45237. This version of the System ROM should be paired with Server Platform Services (SPS) Firmware 06.00.03.604 (2.00_12_20_2023).

Deliverable Name:

HPE ProLiant ML30 Gen10 Plus System ROM - U61

Release Version:

2.00_02-01-2024

Last Recommended or Critical Revision:

2.00_02-01-2024

Previous Revision:

1.90_10-19-2023

Firmware Dependencies:

Enhancements/New Features:

Added new Microsoft secure boot keys, KEK2023, Microsoft UEFI CA 2023 and Windows UEFI CA 2023, since the original keys will expire in 2026.

Corrected Redfish Property value changed from vN_N_N to N.N.N in uri:

/redfish/v1/registrystore/registries/{lang}/biosattributeregistry{Platform}.vN_N_N

there, {lang} = { en, ja, zh }, {platform} = Platform Name e.g. A55, U63 , vN_N_N =

version number defined as Redfish specification

[Example]

uri: /redfish/v1/registrystore/registries/zh/biosattributeregistrya55.v1_1_20

Property of RegistryVersion is changed from v1_1_20 to 1.1.20

Added the System Configuration (RBSU) option "Boot Options/UEFI Boot Settings/Filter Non-bootable Drives" and set to "Auto" by default. This setting has the following Redfish property:

/redfish/v1/systems/1/bios/settings/FilterNonbootableDrive

Problems Fixed:

This revision of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2024.1 guidance.

This revision of the System ROM includes the mitigation for vulnerabilities documented as CVE-2021-38575, CVE-2023-45853, CVE-2022-36763 and CVE-2022-36764.

This revision of the System ROM includes the mitigation for NetworkPkg PXE IP stack vulnerabilities documented as CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, and CVE-2023-45237.

Addressed an issue where the operating system cannot detect the iSCSI hard drive through IPv6 installation if the iSCSI IpAddressType is set to auto.

Addressed an issue where DmiAspmCtrl was not set accordingly when setting DMI ASPM to Disabled/L1 Enabled.

Known Issues:

Fixes

Important Notes:

This revision of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2024.1 guidance. This revision of the System ROM includes the mitigation for vulnerabilities documented as CVE-2021-38575, CVE-2023-45853, CVE-

2022-36763 and CVE-2022-36764. This revision of the System ROM includes the mitigation for NetworkPkg PXE IP stack vulnerabilities documented as CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, and CVE-2023-45237. This version of the System ROM should be paired with Server Platform Services (SPS) Firmware 06.00.03.604 (2.00_12_20_2023).

Firmware Dependencies:

Problems Fixed:

This revision of the System ROM contains updates aligned with the Intel Product Update (IPU) version IPU.2024.1 guidance.

This revision of the System ROM includes the mitigation for vulnerabilities documented as CVE-2021-38575, CVE-2023-45853, CVE-2022-36763 and CVE-2022-36764.

This revision of the System ROM includes the mitigation for NetworkPkg PXE IP stack vulnerabilities documented as CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, and CVE-2023-45237.

Addressed an issue where the operating system cannot detect the iSCSI hard drive through IPv6 installation if the iSCSI IpAddressType is set to auto.

Addressed an issue where DmiAspmCtrl was not set accordingly when setting DMI ASPM to Disabled/L1 Enabled.

Known Issues:

Enhancements

Added new Microsoft secure boot keys, KEK2023, Microsoft UEFI CA 2023 and Windows UEFI CA 2023, since the original keys will expire in 2026.

Corrected Redfish Property value changed from vN_N_N to N.N.N in uri:

/redfish/v1/registrystore/registries/{lang}/biosattributeregistry{Platform}.vN_N_N

there, {lang} = { en, ja, zh }, {platform} = Platform Name e.g. A55, U63 , vN_N_N =

version number defined as Redfish specification

[Example]

uri: /redfish/v1/registrystore/registries/zh/biosattributeregistrya55.v1_1_20

Property of RegistryVersion is changed from v1_1_20 to 1.1.20

Added the System Configuration (RBSU) option "Boot Options/UEFI Boot Settings/Filter Non-bootable Drives" and set to "Auto" by default. This setting has the following Redfish property:

/redfish/v1/systems/1/bios/settings/FilterNonbootableDrive

ROM Flash Firmware Package - HPE ProLiant ML350 Gen10 (U41) Servers
Version: 3.10_02-22-2024 **(Recommended)**
Filename: U41_3.10_02_22_2024.fwpkg

Important Note!

Important Notes:

This version of the System ROM should be paired with Server Platform Services (SPS) Firmware 04.01.05.002.

Deliverable Name:

HPE ProLiant ML350 Gen10 System ROM - U41

Release Version:

3.10_02-22-2024

Last Recommended or Critical Revision:

3.10_02-22-2024

Previous Revision:

3.00_10-19-2023

Firmware Dependencies:

None

Enhancements/New Features:

Patch for CVE-2021-38575: The vulnerability allows a remote attacker to execute arbitrary code on the target system.

Patch the primary APIC ID for SMBIOS type 211: Some special CPUs may not have an intra-processor APIC ID == 00h and may cause wrong TControl data.

Patch for CVE-2023-45853: The vulnerability allows a remote attacker to execute arbitrary code on the target system.

The vulnerability exists due to a boundary error in the IScsiHexToBin() function in NetworkPkg/IScsiDxe. A remote attacker with ability to inject data into communication between edk2 and the iSCSI target can execute arbitrary code on the target system.

Prevented a non-standard VPD content from causing the UEFI read function to become write.

Patch for CVE-2022-36763 and CVE-2022-36764: EDK2 is susceptible to a vulnerability in the Tcg2MeasureGptTable() function, allowing a user to trigger a heap buffer overflow via a local network. Successful exploitation of this vulnerability may result in a compromise of confidentiality, integrity, and/or availability.

Added a new event support for IML.

Patch for CVE-2023-45229: EDK2 NetworkPkg Vulnerability

Added an additional retry mechanisms to avoid a BIOS hang from iLO failure.

Corrected Redfish Property value changed from vN_N_N to N.N.N in uri:

/redfish/v1/registrystore/registries/{lang}/biosattributeregistry{Platform}.vN_N_N

there, {lang} = { en, ja, zh }, {platform} = Platform Name e.g. A55, U63 , vN_N_N =

version number defined as Redfish specification

[Example]

uri: /redfish/v1/registrystore/registries/zh/biosattributeregistrya55.v1_1_20

Property of RegistryVersion is changed from v1_1_20 to 1.1.20

Problems Fixed:

Addressed an issue where SBCE and ECC storm records may disappear from AHS.

Addressed an issue where the iSCSI SW IPv6 HDD is not found under OS when the iSCSI IpAddressType is set to Auto.

Addressed an issue where the server may hang due to an IE function error.

Merged the solutions from EDK2 for vulnerabilities:

- Buffer overflow in the DHCPv6 client via a long Server ID option

- Out-of-bounds read when handling a ND Redirect message with truncated options

- Infinite loop when parsing unknown options in the Destination Options header

- Infinite loop when parsing a PadN option in the Destination Options header

- Buffer overflow when processing DNS Servers option in a DHCPv6 Advertise message

- Predictable TCP ISNs

- Use of a Weak PseudoRandom Number Generator

Known Issues:

None

Fixes

Important Notes:

This version of the System ROM should be paired with Server Platform Services (SPS) Firmware 04.01.05.002.

Firmware Dependencies:

None

Problems Fixed:

Addressed an issue where SBCE and ECC storm records may disappear from AHS.

Addressed an issue where the iSCSI SW IPv6 HDD is not found under OS when the iSCSI IpAddressType is set to Auto.

Addressed an issue where the server may hang due to an IE function error.

Merged the solutions from EDK2 for vulnerabilities:

- Buffer overflow in the DHCPv6 client via a long Server ID option

- Out-of-bounds read when handling a ND Redirect message with truncated options

- Infinite loop when parsing unknown options in the Destination Options header

- Infinite loop when parsing a PadN option in the Destination Options header

- Buffer overflow when processing DNS Servers option in a DHCPv6 Advertise message

- Predictable TCP ISNs

- Use of a Weak PseudoRandom Number Generator

Known Issues:

None

Enhancements

Patch for CVE-2021-38575: The vulnerability allows a remote attacker to execute arbitrary code on the target system.

Patch the primary APIC ID for SMBIOS type 211: Some special CPUs may not have an intra-processor APIC ID == 00h and may cause wrong TControl data.

Patch for CVE-2023-45853: The vulnerability allows a remote attacker to execute arbitrary code on the target system.

The vulnerability exists due to a boundary error in the IScsiHexToBin() function in NetworkPkg/IScsiDxe. A remote attacker with ability to inject data into communication between edk2 and the iSCSI target can execute arbitrary code on the target system.

Prevented a non-standard VPD content from causing the UEFI read function to become write.

Patch for CVE-2022-36763 and CVE-2022-36764: EDK2 is susceptible to a vulnerability in the Tcg2MeasureGptTable() function, allowing a user to trigger a heap buffer overflow via a local network. Successful exploitation of this vulnerability may result in a compromise of confidentiality, integrity, and/or availability.

Added a new event support for IML.

Patch for CVE-2023-45229: EDK2 NetworkPkg Vulnerability

Added an additional retry mechanisms to avoid a BIOS hang from iLO failure.

Corrected Redfish Property value changed from vN_N_N to N.N.N in uri:

/redfish/v1/registrystore/registries/{lang}/biosattributeregistry{Platform}.vN_N_N

there, {lang} = { en, ja, zh }, {platform} = Platform Name e.g. A55, U63 , vN_N_N =

version number defined as Redfish specification

[Example]

uri: /redfish/v1/registrystore/registries/zh/biosattributeregistrya55.v1_1_20

Property of RegistryVersion is changed from v1_1_20 to 1.1.20

ROM Flash Universal Firmware Package - HPE ProLiant DL325/DL325 v2/DL345 Gen10 Plus (A43) Servers
Version: 3.00_01-26-2024 **(Recommended)**
Filename: A43_3.00_01_26_2024.fwpkg

Important Note!

Important Notes:

This revision of the System ROM includes AMD reference code MilanPI 1.0.0.C for AMD 3rd Generation EPYC processors. This revision of the System ROM includes AMD reference code RomePI 1.0.0.H for AMD 2nd Generation EPYC processors. This revision of the System ROM includes the mitigation for security vulnerabilities CVE-2023-31346 and CVE-2023-31347 for AMD 3rd Generation EPYC processors. This security vulnerability is documented in the CVE report site. This issue is not unique to HPE servers. This revision of the System ROM includes the mitigation for NetworkPkg iSCSI Dxe driver vulnerability documented as CVE-2021-38575. This revision of the System ROM includes the mitigation for NetworkPkg PXE IP stack vulnerabilities documented as CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, and CVE-2023-45237.

Deliverable Name:

HPE ProLiant DL325/DL325 v2/DL345 Gen10 Plus System ROM - A43

Release Version:

3.00_01_26_2024

Last Recommended or Critical Revision:

3.00_01_26_2024

Previous Revision:

2.90_10-27-2023

Firmware Dependencies:

None

Enhancements/New Features:

Added new Microsoft secure boot keys, KEK2023, Microsoft UEFI CA 2023 and Windows UEFI CA 2023, since the original keys will expire in 2026.

Added the System Configuration (RBSU) option "Boot Options/UEFI Boot Settings/Filter Non-bootable Drives" and set to "Auto" by default. This setting has the following Redfish property:

/redfish/v1/systems/1/bios/settings/FilterNonbootableDrive

Problems Fixed:

This revision of the System ROM includes the mitigation for security vulnerabilities CVE-2023-31346 and CVE-2023-31347 for AMD 3rd Generation EPYC processors. This security vulnerability is documented in the CVE report site. This issue is not unique to HPE servers.

This revision of the System ROM includes the mitigation for NetworkPkg iSCSI Dxe driver vulnerability documented as CVE-2021-38575.

This revision of the System ROM includes the mitigation for NetworkPkg PXE IP stack vulnerabilities documented as CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, and CVE-2023-45237.

Known Issues:

None

Fixes

Important Notes:

This revision of the System ROM includes AMD reference code MilanPI 1.0.0.C for AMD 3rd Generation EPYC processors. This revision of the System ROM includes AMD reference code RomePI 1.0.0.H for AMD 2nd Generation EPYC processors. This revision of the System ROM includes the mitigation for security vulnerabilities CVE-2023-31346 and CVE-2023-31347 for AMD 3rd Generation EPYC processors. This security vulnerability is documented in the CVE report site. This issue is not unique to HPE servers. This revision of the System ROM includes the mitigation for NetworkPkg iSCSI Dxe driver vulnerability documented as CVE-2021-38575. This revision of the System ROM includes the mitigation for NetworkPkg PXE IP stack vulnerabilities documented as CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, and CVE-2023-45237.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the mitigation for security vulnerabilities CVE-2023-31346 and CVE-2023-31347 for AMD 3rd Generation EPYC processors. This security vulnerability is documented in the CVE report site. This issue is not unique to HPE servers.

This revision of the System ROM includes the mitigation for NetworkPkg iSCSI Dxe driver vulnerability documented as CVE-2021-38575.

This revision of the System ROM includes the mitigation for NetworkPkg PXE IP stack vulnerabilities documented as CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, and CVE-2023-45237.

Known Issues:

None

Enhancements

Added new Microsoft secure boot keys, KEK2023, Microsoft UEFI CA 2023 and Windows UEFI CA 2023, since the original keys will expire in 2026.

Added the System Configuration (RBSU) option "Boot Options/UEFI Boot Settings/Filter Non-bootable Drives" and set to "Auto" by default. This setting has the following Redfish property:

/redfish/v1/systems/1/bios/settings/FilterNonbootableDrive

ROM Flash Universal Firmware Package - HPE ProLiant DL360/DL380 Gen10 Plus (U46) Servers
Version: 2.00_03-06-2024 **(Recommended)**
Filename: U46_2.00_03_06_2024.fwpkg

Important Note!

Important Notes:

This version of the System ROM should be paired with Server Platform Services (SPS) Firmware 04.04.04.603 (2.00_12_18_2023).

Deliverable Name:

HPE ProLiant DL360/DL380 Gen10 Plus System ROM - U46

Release Version:

2.00_03-06-2024

Last Recommended or Critical Revision:

2.00_03-06-2024

Previous Revision:

1.90_10-19-2023

Firmware Dependencies:

None

Enhancements/New Features:

Enhanced the SMBIOS type 203 ability for PCI device information displays that can support when the PCI slot is bifurcated.

Added an option of "Filter Non-bootable Drives" in RBSU Boot Options.

Problems Fixed:

Addressed an issue where the PCI VPD data would be written unconditionally while system is accessing to PCI VPD.
This revision of the System ROM includes the latest revision of the Intel IPU 2024.1 BIOS update which provides Intel's mitigation for BIOS advisory and security vulnerabilities documented as CVE-2021-38575, CVE-2022-36763, CVE-2022-36764, CVE-2023-45229 and CVE-2023-45853. This security vulnerability is documented in the CVE report site. This issue is not unique to HPE servers.
Addressed an issue where the UBM version between RBSU and iLO web pages was not synchronized.
Addressed an issue where NVME hot plug when installing fully loaded NVME drives.
Addressed a potential security vulnerability in some 3rd and 4th Generation Intel® Xeon® Processors when using Intel® Software Guard Extensions (SGX) or Intel® Trust Domain Extensions (TDX) may allow escalation of privilege, as documented in CVE-2023-22655.
Addressed an issue vulnerabilities in network IP stack documented as from CVE-2023-45230 to CVE-2023-45237.
Addressed an issue where the PCIE slot control would disappear in RBSU when the PCIE switchboard is installed in the system.
Addressed an issue where the iSCSI SW ipv6 HDD could not be found under OS when iSCSI IP Address Type option is set to Auto in RBSU Network Options / iSCSI Configuration / Add an iSCSI Attempt > select Network device > IP Address Type.
Addressed an issue where setup options of the BIOS Configuration (RBSU) utility may not be synchronized to the latest state when a server is idle in RBSU for more than 30 minutes.

Known Issues:

None

Fixes

Important Notes:

This version of the System ROM should be paired with Server Platform Services (SPS) Firmware 04.04.04.603 (2.00_12_18_2023).

Firmware Dependencies:

None

Problems Fixed:

Addressed an issue where the PCI VPD data would be written unconditionally while system is accessing to PCI VPD.
This revision of the System ROM includes the latest revision of the Intel IPU 2024.1 BIOS update which provides Intel's mitigation for BIOS advisory and security vulnerabilities documented as CVE-2021-38575, CVE-2022-36763, CVE-2022-36764, CVE-2023-45229 and CVE-2023-45853. This security vulnerability is documented in the CVE report site. This issue is not unique to HPE servers.
Addressed an issue where the UBM version between RBSU and iLO web pages was not synchronized.
Addressed an issue where NVME hot plug when installing fully loaded NVME drives.
Addressed a potential security vulnerability in some 3rd and 4th Generation Intel® Xeon® Processors when using Intel® Software Guard Extensions (SGX) or Intel® Trust Domain Extensions (TDX) may allow escalation of privilege, as documented in CVE-2023-22655.
Addressed an issue vulnerabilities in network IP stack documented as from CVE-2023-45230 to CVE-2023-45237.
Addressed an issue where the PCIE slot control would disappear in RBSU when the PCIE switchboard is installed in the system.
Addressed an issue where the iSCSI SW ipv6 HDD could not be found under OS when iSCSI IP Address Type option is set to Auto in RBSU Network Options / iSCSI Configuration / Add an iSCSI Attempt > select Network device > IP Address Type.
Addressed an issue where setup options of the BIOS Configuration (RBSU) utility may not be synchronized to the latest state when a server is idle in RBSU for more than 30 minutes.

Known Issues:

None

Enhancements

Enhanced the SMBIOS type 203 ability for PCI device information displays that can support when the PCI slot is bifurcated.

Added an option of "Filter Non-bootable Drives" in RBSU Boot Options.

ROM Flash Universal Firmware Package - HPE ProLiant DL365/DL385/DL385 v2 Gen10 Plus (A42) Servers
Version: 3.00_01-26-2024 **(Recommended)**
Filename: A42_3.00_01_26_2024.fwpkg

Important Note!

Important Notes:

This revision of the System ROM includes AMD reference code MilanPI 1.0.0.C for AMD 3rd Generation EPYC processors. This revision of the System ROM includes AMD reference code RomePI 1.0.0.H for AMD 2nd Generation EPYC processors. This revision of the System ROM includes the mitigation for security vulnerabilities CVE-2023-31346 and CVE-2023-31347 for AMD 3rd Generation EPYC processors. This security vulnerability is documented in the CVE report site. This issue is not unique to HPE servers. This revision of the System ROM includes the mitigation for NetworkPkg iSCSI Dxe driver vulnerability documented as CVE-2021-38575. This revision of the System ROM includes the mitigation for NetworkPkg PXE IP stack vulnerabilities documented as CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, and CVE-2023-45237.

Deliverable Name:

HPE DL365 Gen10 Plus/DL385 Gen10 Plus/DL385 v2 Gen10 Plus System ROM - A42

Release Version:

3.00_01_26_2024

Last Recommended or Critical Revision:

3.00_01_26_2024

Previous Revision:

2.90_10-27-2023

Firmware Dependencies:

None

Enhancements/New Features:

Added new Microsoft secure boot keys, KEK2023, Microsoft UEFI CA 2023 and Windows UEFI CA 2023, since the original keys will expire in 2026.

Added the System Configuration (RBSU) option "Boot Options/UEFI Boot Settings/Filter Non-bootable Drives" and set to "Auto" by default. This setting has the following Redfish property:

/redfish/v1/systems/1/bios/settings/FilterNonbootableDrive

Problems Fixed:

This revision of the System ROM includes the mitigation for security vulnerabilities CVE-2023-31346 and CVE-2023-31347 for AMD 3rd Generation EPYC processors. This security vulnerability is documented in the CVE report site. This issue is not unique to HPE servers.

This revision of the System ROM includes the mitigation for NetworkPkg iSCSI Dxe driver vulnerability documented as CVE-2021-38575.

This revision of the System ROM includes the mitigation for NetworkPkg PXE IP stack vulnerabilities documented as CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, and CVE-2023-45237.

Known Issues:

None

Fixes

Important Notes:

This revision of the System ROM includes AMD reference code MilanPI 1.0.0.C for AMD 3rd Generation EPYC processors. This revision of the System ROM includes AMD reference code RomePI 1.0.0.H for AMD 2nd Generation EPYC processors. This revision of the System ROM includes the mitigation for security vulnerabilities CVE-2023-31346 and CVE-2023-31347 for AMD 3rd Generation EPYC processors. This security vulnerability is documented in the CVE report site. This issue is not unique to HPE servers. This revision of the System ROM includes the mitigation for NetworkPkg iSCSI Dxe driver vulnerability documented as CVE-2021-38575. This revision of the System ROM includes the mitigation for NetworkPkg PXE IP stack vulnerabilities documented as CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, and CVE-2023-45237.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the mitigation for security vulnerabilities CVE-2023-31346 and CVE-2023-31347 for AMD 3rd Generation EPYC processors. This security vulnerability is documented in the CVE report site. This issue is not unique to HPE servers.

This revision of the System ROM includes the mitigation for NetworkPkg iSCSI Dxe driver vulnerability documented as CVE-2021-38575.

This revision of the System ROM includes the mitigation for NetworkPkg PXE IP stack vulnerabilities documented as CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, and CVE-2023-45237.

Known Issues:

None

Enhancements

Added new Microsoft secure boot keys, KEK2023, Microsoft UEFI CA 2023 and Windows UEFI CA 2023, since the original keys will expire in 2026.

Added the System Configuration (RBSU) option "Boot Options/UEFI Boot Settings/Filter Non-bootable Drives" and set to "Auto" by default. This setting has the following Redfish property:

/redfish/v1/systems/1/bios/settings/FilterNonbootableDrive

Driver - Lights-Out Management Top

HPE iLO Native Driver for ESXi 7.0
Version: 10.8.2 **(Recommended)**
Filename: ilo-driver_700.10.8.2.2-1OEM.700.1.0.15843807_22942561.zip

Fixes

This product addressed a memory leak in vmkernel.

Driver - Network Top

HPE Intel i40en Driver for VMware vSphere 8.0

Version: 2023.10.00 **(Recommended)**
Filename: cp058385.compsig; cp058385.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 3.22.0 or later, for use with this driver.

Enhancements

This product enhanced the compatibility with firmware of Fortville 9.3.

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 563i Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMSFP+ Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMT Adapter
- HPE Ethernet 10Gb 2-port 568i Adapter
- HPE Ethernet 10Gb 2-port SFP+ OCP3 X710-DA2 Adapter
- HPE Ethernet 10Gb 2-port SFP+ X710-DA2 Adapter

HPE Intel igbn Driver for VMware vSphere 8.0
Version: 2023.09.00 **(Recommended)**
Filename: cp056804.compsig; cp056804.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 3.21.0 or later, for use with this driver.

Fixes

This product fix an issue that TCP traffic on VMs might be interrupted if PF undergoes a reset.

Supported Devices and Features

These drivers support the following network adapters:

- HPE Ethernet 1Gb 2-port 361T Adapter
- HPE Ethernet 1Gb 2-port 361i Adapter
- HPE Ethernet 1Gb 2-port 363i Adapter
- HPE Ethernet 1Gb 4-port 366FLR Adapter
- HPE Ethernet 1Gb 4-port 366T Adapter
- HPE Ethernet 1Gb 4-port 366i Adapter
- HPE Ethernet 1Gb 4-port 366i Communication Board
- Intel I350-T4 Ethernet 1Gb 4-port BASE-T Adapter for HPE
- Intel I350-T4 Ethernet 1Gb 4-port BASE-T OCP3 Adapter for HPE
- Intel(R) I350 Gigabit Network Connection

HPE Intel ixgben Driver for VMware vSphere 8.0
Version: 2023.09.00 **(Recommended)**
Filename: cp056805.compsig; cp056805.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 3.21.0 or later, for use with this driver.

Fixes

This product fix an issue that TCP traffic on VMs might be interrupted if PF undergoes a reset.

Enhancements

This product updated the copyright information and compatibility with firmware

Supported Devices and Features

These drivers support the following network adapters:

- HPE Ethernet 10Gb 2-port 560SFP+ Adapter
- HPE Ethernet 10Gb 2-port 560FLR-SFP+ Adapter
- HPE Ethernet 10Gb 2-port 561T Adapter
- HPE Ethernet 10Gb 2-port 561FLR-T Adapter
- HPE Ethernet 10Gb 2-port 562T Adapter
- HPE Ethernet 10Gb 2-port 562FLR-T Adapter

HPE QLogic FastLinQ 10/25/50 GbE Multifunction Driver for VMware vSphere 8.0
Version: 2024.03.00 **(Recommended)**
Filename: cp058994.compsig; cp058994.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 as below for use with these drivers,

- HPE QLogic FastLinQ Firmware Package for Arrowhead adapters, version 8.65.09 or later.
- HPE QLogic FastLinQ Online Firmware Upgrade Utility for VMware, version 4.18.50 or later.

Fixes

This product correct an issue which fixed PSOD that keep DRSS module parameter disabled.

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 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

HPE QLogic NX2 10/20 GbE Multifunction Driver for VMware vSphere 8.0
Version: 2024.03.00 **(Recommended)**
Filename: cp058996.compsig; cp058996.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 QLogic NX2 Online Firmware Upgrade Utility for VMware*, version 1.34.0 or later, for use with this driver.

Enhancements

This product enhanced the compatibility with VMware firmware component 1.34.0.

Supported Devices and Features

These drivers support the following network adapters:

- HPE Ethernet 10Gb 2-port 530T Adapter
- HPE Ethernet 10Gb 2-port 530SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 533FLR-T Adapter
- HPE FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 4-port 536FLR-T Adapter

Intel icen Driver for VMware vSphere 8.0
Version: 2023.10.00 **(Recommended)**
Filename: cp058387.compsig; cp058387.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 *Intel Firmware Package For E810 Ethernet Adapter*, version 4.30 or later, for use with these drivers.

Fixes

- This product correct an issue which fixes PSOD that the Netdump fail to sent to target vCenter Server.
- This product correct an issue which fixes high pNIC error that triggered by driver reporting EIPE error is a false alarm.

Supported Devices and Features

This product supports the following network adapters:

- Intel E810-CQDA2 Ethernet 100Gb 2-port QSFP28 Adapter for HPE
- Intel E810-CQDA2 Ethernet 100Gb 2-port QSFP28 OCP3 Adapter for HPE
- Intel E810-XXVDA4 Ethernet 10/25Gb 4-port SFP28 Adapter for HPE
- Intel E810-XXVDA2 Ethernet 10/25Gb 2-port SFP28 Adapter for HPE
- Intel E810-XXVDA2 Ethernet 10/25Gb 2-port SFP28 OCP3 Adapter for HPE
- Intel E810-2CQDA2 Ethernet 100Gb 2-port QSFP28 Adapter for HPE
- Intel E810-XXVDA4 Ethernet 10/25Gb 4-port SFP28 OCP3 Adapter for HPE

Driver - Storage Controller Top

HPE MR416i-p, MR416i-o, MR216i-o, MR408i-o, MR216i-p Gen10P and Gen11 controller (64-bit) Driver for vSphere 8.0
Version: 2023.12.01 **(Recommended)**
Filename: cp057484.compsig; cp057484.zip

Important Note!

- **This new 7.26 release have not completed vSAN certification, please don't update for vSAN environment for now. Target to complete vSAN certification by end of February 2024.**
- This component is intended to be used by HPE applications. It is a zip that contains the same driver deliverable available from the vmware.com and the HPE vibsdepot.hpe.com webpages, plus an HPE specific CPXXXX.xml file.

Enhancements

- New release for version 7.726.02.00.
- This new 7.26 release have not completed vSAN certification, please don't update for vSAN environment for now. Target to complete vSAN certification by end of February 2024.

HPE ProLiant Gen10 Smart Array and Gen10 Plus and Gen11 Smart RAID Controller Driver for VMware vSphere 8.0 (Driver Component).
Version: 2024.04.01 **(Recommended)**
Filename: cp058434.compsig; cp058434.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

vmware.com, plus an HPE specific CPXXXX.xml file.

Enhancements

- Made changes to enhance the testability of the driver. Changes do not impact end customers.

Firmware - Network Top

HPE Broadcom NetXtreme-E Online Firmware Upgrade Utility for VMware
Version: 216.0.33011 **(Recommended)**
Filename: CP058229.compsig; CP058229.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 Intel Online Firmware Upgrade Utility VMware for HPE ProLiant Gen9 and Gen10 server series Only.
Version: 3.22.0 **(Recommended)**
Filename: CP058405.compsig; CP058405.zip

Important Note!

- **This component ONLY support HPE ProLiant Gen9 and Gen10 server series.**

This software package contains the following firmware versions for the below listed supported network adapters:

NIC	EEPROM/NVM Version	OROM Version	Single NVM Version
HPE Ethernet 1Gb 2-port 361T Adapter	80001147	1.3437.0	N/A
HPE Ethernet 1Gb 4-port 366FLR Adapter	800011A1	1.3437.0	N/A
HPE Ethernet 1Gb 4-port 366T Adapter	800011F1	1.3437.0	N/A
HPE Ethernet 1Gb 2-port 368i Adapter	80003AC5	1.3437.0	N/A
HPE Ethernet 1Gb 2-port 368FLR-MMT Adapter	80003AC2	1.3437.0	N/A
HPE Ethernet 1Gb 4-port 369i Adapter	80003AC3	1.3437.0	N/A
HPE Ethernet 10Gb 2-port 568i Adapter	80003AC4	1.3437.0	N/A
HPE Ethernet 10Gb 2-port 568FLR-MMSFP+ Adapter	80003AC2	1.3437.0	N/A
HPE Ethernet 10Gb 2-port 568FLR-MMT Adapter	80003AC2	1.3437.0	N/A
HPE Ethernet 10Gb 2-port 563i Adapter	800035C0	1.3437.0	N/A
HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter	8000E3EC	1.3437.0	11.1.5
HPE Ethernet 10Gb 2-port 562FLR-T Adapter	800016F1	1.3437.0	10.55.3
HPE Ethernet 10Gb 2-port 562SFP+ Adapter	8000E3EB	1.3437.0	11.1.5
HPE Ethernet 10Gb 2-port 562T Adapter	800016EF	1.3437.0	10.55.3

The combo image v1.3437.0 includes: Boot Agent: 1GbE - v1.5.90, 10GbE - v2.4.51, 40GbE - v1.1.44 & UEFI Drivers: 1GbE - v9.8.33, 10GbE - v8.2.13, 40GbE - v4.9.70

Single NVM Version is new firmware format which represent an unified version in place of the previously used EEPROM/NVM Version or OROM version.

This software package no longer contains Firmware for the below listed supported network adapters:

HPE Ethernet 1Gb 2-port 361i Adapter

HPE Ethernet 1Gb 2-port 363i Adapter

HPE Ethernet 1Gb 4-port 366i Adapter

HPE Ethernet 1Gb 4-port 366i Communication Board

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

HPE Ethernet 10Gb 2-port 560SFP+ Adapter

HPE Ethernet 10Gb 2-port 561FLR-T Adapter

HPE Ethernet 10Gb 2-port 561T Adapter

- The latest firmware version of above adapters, please refer to the link : https://support.hpe.com/connect/s/softwaredetails?language=en_US&softwareId=MTX_4e84847286af4760911448c7a0&tab=releaseNote

Prerequisites

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

Fixes

This product addresses an issue where running the firmware update command (./Execute_Component -s) only updates the OROM.

Enhancements

This product enhanced the compatibility with the latest drivers.

Supported Devices and Features

This package supports the following network adapters:

- HPE Ethernet 1Gb 2-port 361T Adapter
- HPE Ethernet 1Gb 2-port 368FLR-MMT Adapter
- HPE Ethernet 1Gb 2-port 368i Adapter
- HPE Ethernet 1Gb 4-port 366FLR Adapter
- HPE Ethernet 1Gb 4-port 366T Adapter
- HPE Ethernet 1Gb 4-port 369i Adapter
- HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter
- HPE Ethernet 10Gb 2-port 562FLR-T Adapter
- HPE Ethernet 10Gb 2-port 562SFP+ Adapter
- HPE Ethernet 10Gb 2-port 562T Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMSFP+ Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMT Adapter
- HPE Ethernet 10Gb 2-port 568i Adapter
- HPE Ethernet 10Gb 2-port 563i Adapter

HPE QLogic FastLinQ Firmware Package for Arrowhead adapters
Version: 8.65.09 (B) **(Recommended)**
Filename: ql_hp_ah_mbi_8.65.09_pldm.fwpkg

Important Note!

For Firmware installation, there is no OS and drivers dependency.
For Firmware compatibility during production, HPE recommends the drivers for use with the firmware Package product as below,

- HPE QLogic FastLinQ 10/25/50 GbE Drivers for Linux, version 8.74.0.1-1 or later
- HPE QLogic FastLinQ 10/25/50 GbE Drivers for Microsoft Windows Server x64 Editions, version 8.72.11.0 or later
- HPE QLogic FastLinQ 10/25/50 GbE Multifunction Drivers for VMware, version 2024.03.00 or later

This software package contains combo image v8.65.09. This combo image includes: Boot Code (MFW): 8.65.4.0, PXE:2.0.19, and UEFI: 4.1.13.1.

Fixes

This product addresses the issue of inconsistent metadata within the component products.

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 Adapter
- HPE StoreFabric CN1200R-T Converged Network Adapter
- HPE StoreFabric CN1300R Converged Network Adapter

HPE QLogic FastLinQ Online Firmware Upgrade Utility for VMware
Version: 4.18.50 **(Recommended)**
Filename: CP058191.compsig; CP058191.zip

Important Note!

HPE recommends *HPE QLogic FastLinQ 10/25/50GbE Multifunction Drivers for VMware*, versions 2023.12.00 or later, for use with this firmware.

This software package contains combo image version v8.65.09 includes:

- Boot Code (MFW): 8.65.4.0
- UEFI: 4.1.13.1
- 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 addresses an issue where BSOD is seen.

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 Online Firmware Upgrade Utility for VMware
Version: 1.34.0 **(Recommended)**
Filename: CP059079.compsig; CP059079.zip

Important Note!

HPE recommends HPE QLogic NX2 10/20GbE Multifunction Drivers for VMware, versions 2024.03.00 or later, for use with this firmware.

This software package contains combo image v7.19.21 with the following firmware versions:

NIC	Boot Code Version	PXE Version	UEFI Version	iSCSI Version	FCoE Version	CCM Version	L2 Version
HPE Ethernet 10Gb 2-port 530SFP+ Adapter HPE Ethernet 10Gb 2-port 530T Adapter	7.16.14	7.14.13	8.9.3	n/a	n/a	7.14.4	7.12.25
HPE Ethernet 10Gb 2-port 533FLR-T Adapter HPE FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter HPE FlexFabric 10Gb 4-port 536FLR-T Adapter	7.16.14	7.14.13	8.9.3	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 addresses an issue that FCoE Boot Target issue.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 530SFP+ Adapter
- HPE Ethernet 10Gb 2-port 530T Adapter
- HPE Ethernet 10Gb 2-port 533FLR-T Adapter
- HPE FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 4-port 536FLR-T Adapter

Intel Firmware Package For E810-2CQDA2 Ethernet 100Gb 2-port QSFP28 Adapter
Version: 4.30 **(Recommended)**
Filename: HPE_E810_2CQDA2_O_SEC_4p30_PLDMoMCTP_8001AF25.fwpkg

Important Note!

For Firmware installation, there is no OS and drivers dependency.
For Firmware compatibility during production, HPE recommends the drivers for use with the firmware Package product as below,

- Intel icea Driver for Microsoft Windows Server, version 1.13.242.0 or later
- Intel ice Drivers for Linux, version 1.12.6-1 or later
- Intel icen Driver for VMware, version 2023.10.00 or later

This FW version does not support Port.Reset RDE metrics. This product will be enhance to improve the functions in the future release

Enhancements

This product enhanced the compatibility with icea driver.

Supported Devices and Features

This product supports the following network adapters:

- Intel E810-2CQDA2 Ethernet 100Gb 2-port QSFP28 Adapter for HPE

Intel Firmware Package For E810-CQDA2 Ethernet 100Gb 2-port QSFP28 Adapter
Version: 4.30 **(Recommended)**
Filename: HPE_E810_CQDA2_4p30_PLDMoMCTP_8001AF29.fwpkg

Important Note!

For Firmware installation, there is no OS and drivers dependency.
For Firmware compatibility during production, HPE recommends the drivers for use with the firmware Package product as below,

- Intel icea Driver for Microsoft Windows Server, version 1.13.242.0 or later
- Intel ice Drivers for Linux, version 1.12.6-1 or later
- Intel icen Driver for VMware, version 2023.10.00 or later

This FW version does not support Port.Reset RDE metrics. This product will be enhance to improve the functions in the future release

Enhancements

This product enhanced the compatibility with icea driver.

Supported Devices and Features

This product supports the following network adapters:

- Intel E810-CQDA2 Ethernet 100Gb 2-port QSFP28 Adapter for HPE

Intel Firmware Package For E810-CQDA2 Ethernet 100Gb 2-port QSFP28 OCP3 Adapter
Version: 4.30 **(Recommended)**
Filename: HPE_E810_CQDA2_OCP_4p30_NCSIwPLDMoMCTP_8001AF24.fwpkg

Important Note!

For Firmware installation, there is no OS and drivers dependency.
For Firmware compatibility during production, HPE recommends the drivers for use with the firmware Package product as below,

- Intel icea Driver for Microsoft Windows Server, version 1.13.242.0 or later
- Intel ice Drivers for Linux, version 1.12.6-1 or later
- Intel icen Driver for VMware, version 2023.10.00 or later

This FW version does not support Port.Reset RDE metrics. This product will be enhance to improve the functions in the future release

Enhancements

This product enhanced the compatibility with icea driver.

Supported Devices and Features

This product supports the following network adapters:

- Intel E810-CQDA2 Ethernet 100Gb 2-port QSFP28 OCP3 Adapter for HPE

Intel Firmware Package For E810-XXVDA2 Ethernet 10/25Gb 2-port SFP28 Adapter
Version: 4.30 **(Recommended)**
Filename: HPE_E810_XXVDA2_SD_4p30_PLDMoMCTP_8001AF27.fwpkg

Important Note!

For Firmware installation, there is no OS and drivers dependency.
For Firmware compatibility during production, HPE recommends the drivers for use with the firmware Package product as below,

- Intel icea Driver for Microsoft Windows Server, version 1.13.242.0 or later
- Intel ice Drivers for Linux, version 1.12.6-1 or later
- Intel icen Driver for VMware, version 2023.10.00 or later

This FW version does not support Port.Reset RDE metrics. This product will be enhance to improve the functions in the future release

Enhancements

This product enhanced the compatibility with icea driver.

Supported Devices and Features

This product supports the following network adapters:

- Intel E810-XXVDA2 Ethernet 10/25Gb 2-port SFP28 Adapter for HPE

Intel Firmware Package For E810-XXVDA2 Ethernet 10/25Gb 2-port SFP28 OCP3 Adapter
Version: 4.30 **(Recommended)**
Filename: HPE_E810_XXVDA2_SD_OCP_4p30_NCSIwPLDMoMCTP_8001AF23.fwpkg

Important Note!

For Firmware installation, there is no OS and drivers dependency.
For Firmware compatibility during production, HPE recommends the drivers for use with the firmware Package product as below,

- Intel icea Driver for Microsoft Windows Server, version 1.13.242.0 or later
- Intel ice Drivers for Linux, version 1.12.6-1 or later
- Intel icen Driver for VMware, version 2023.10.00 or later

This FW version does not support Port.Reset RDE metrics. This product will be enhance to improve the functions in the future release

Enhancements

This product enhanced the compatibility with icea driver.

Supported Devices and Features

This product supports the following network adapters:

- Intel E810-XXVDA2 Ethernet 10/25Gb 2-port SFP28 OCP3 Adapter for HPE

Intel Firmware Package For E810-XXVDA4 Ethernet 10/25Gb 4-port SFP28 Adapter
Version: 4.30 **(Recommended)**
Filename: HPE_E810_XXVDA4_FH_4p30_PLDMoMCTP_8001AF35.fwpkg

Important Note!

For Firmware installation, there is no OS and drivers dependency.
For Firmware compatibility during production, HPE recommends the drivers for use with the firmware Package product as below,

- Intel icea Driver for Microsoft Windows Server, version 1.13.242.0 or later
- Intel ice Drivers for Linux, version 1.12.6-1 or later
- Intel icen Driver for VMware, version 2023.10.00 or later

This FW version does not support Port.Reset RDE metrics. This product will be enhance to improve the functions in the future

release

Enhancements

This product enhanced the compatibility with icea driver.

Supported Devices and Features

This product supports the following network adapters:

- Intel E810-XXVDA4 Ethernet 10/25Gb 4-port SFP28 Adapter for HPE

Intel Firmware Package For E810-XXVDA4 Ethernet 10/25Gb 4-port SFP28 OCP3 Adapter
Version: 4.30 **(Recommended)**
Filename: HPE_E810_XXV4_OCP_4p30_NCSIwPLDMoMCTP_8001AF22.fwpkg

Important Note!

For Firmware installation, there is no OS and drivers dependency.
For Firmware compatibility during production, HPE recommends the drivers for use with the firmware Package product as below,

- Intel icea Driver for Microsoft Windows Server, version 1.13.242.0 or later
- Intel ice Drivers for Linux, version 1.12.6-1 or later
- Intel icen Driver for VMware, version 2023.10.00 or later

This FW version does not support Port.Reset RDE metrics. This product will be enhance to improve the functions in the future release

Enhancements

This product enhanced the compatibility with icea driver.

Supported Devices and Features

This product supports the following network adapters:

- Intel E810-XXVDA4 Ethernet 10/25Gb 4-port SFP28 OCP3 Adapter for HPE

Intel Online Firmware Upgrade Utility for VMware
Version: 3.22.0 **(Recommended)**
Filename: CP058408.compsig; CP058408.zip

Important Note!

This software package contains the following firmware versions for the below listed supported network adapters:

NIC	EEPROM/NVM Version	OROM Version	NVM Version
HPE Ethernet 10Gb 2-port SFP+ OCP3 X710-DA2 Adapter	8000E5DB	1.3429.0	9.3
HPE Ethernet 10Gb 2-port SFP+ X710-DA2 Adapter	8000E5EC	1.3429.0	9.3
Intel I350-T4 Ethernet 1Gb 4-port BASE-T Adapter	800011F8	1.3429.0	N/A
Intel I350-T4 Ethernet 1Gb 4-port BASE-T OCP3 Adapter	800011EF	1.3429.0	N/A
Intel(R) I350 Gigabit Network Connection (2-port)	8000119C	1.3429.0	N/A
Intel(R) I350 Gigabit Network Connection (4-port)	8000119D	1.3429.0	N/A

The combo image v1.3429.0 includes: Boot Agent: 1GbE - v1.5.90, 10GbE - v2.4.51, 40GbE - v1.1.44 & UEFI Drivers: 1GbE - v9.8.33, 10GbE - v8.2.13, 40GbE - v4.9.70

Prerequisites

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

Fixes

This product addresses an issue where running the firmware update command (./Execute_Component -s) only updates the OROM.

Enhancements

This product enhanced the compatibility with the latest drivers.

Supported Devices and Features

This package supports the following network adapters:

- Intel(R) I350 Gigabit Network Connection (2-port)
- Intel(R) I350 Gigabit Network Connection (4-port)
- HPE Ethernet 1Gb 4-port BaseT I350-T4 Adapter
- HPE Ethernet 1Gb 4-port BaseT I350-T4 OCP3 Adapter
- HPE Ethernet 10Gb 2-port SFP+ X710-DA2 OCP3 Adapter
- HPE Ethernet 10Gb 2-port SFP+ X710-DA2 Adapter

Marvell FastLinQ Firmware Package for Arrowhead adapters
Version: 8.65.09 (B) **(Recommended)**
Filename: ql_ah_mbi_open_8.65.09_pldm.fwpkg

Important Note!

For Firmware installation, there is no OS and drivers dependency.
For Firmware compatibility during production, HPE recommends the drivers for use with the firmware Package product as below,

- Marvell FastLinQ 10/25/50 GbE Drivers for Microsoft Windows Server x64 Editions, version 8.72.11.0 or later
- HPE QLogic FastLinQ 10/25/50 GbE Drivers for Linux, version 8.74.0.1-1 or later
- HPE QLogic FastLinQ 10/25/50 GbE Multifunction Drivers for VMware, version 2024.03.00 or later

Fixes

This product addresses the issue of inconsistent metadata within the component products.

Supported Devices and Features

This product supports the following network adapters:

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

Marvell FastLinQ Online Firmware Upgrade Utility for VMware
Version: 8.55.12 **(Recommended)**
Filename: CP058235.compsig; CP058235.zip

Important Note!

This software package contains combo image v8.55.12. This combo image includes:

- PXE: 2.0.19
- Boot Code (MFW): 8.55.22.0
- UEFI: 6.1.8.2

Prerequisites

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

Fixes

- This product contains support PLDM firmware upgrade base improvements.

- This product addresses an overheat issue on the network adapters as below,

  HPE Ethernet 10Gb 2-port BaseT QL41132HLRJ Adapter
  HPE Ethernet 10Gb 2-port BaseT QL41132HQRJ OCP3 Adapter

Enhancements

This product now supported NPAR enabling option.

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

Mellanox Firmware Package (FWPKG) for HPE InfiniBand HDR/Ethernet 200Gb 1-port QSFP56 PCIe4 x16 MCX653105A-HDAT Adapter : HPE part numbers P23664-B21 and P23664-H21
Version: 20.40.1000 **(Recommended)**
Filename: 20_40_1000-MCX653105A-HDA_HPE_Ax.pldm.fwpkg

Important Note!

For PLDM enabled VPI (Virtual Protocol Interconnect) adapters supporting both InfiniBand mode and Ethernet modes, every firmware version is made available in two different formats at HPE.com:

1. HPE signed PLDM Firmware Package (.FWPKG filename extension) updatable via iLO.
2. Firmware binary (.bin filename extension) updatable via mstflint utility from the Operating System.

Choose the appropriate firmware file format based on your preference and what suits your environment.

Disclaimer: Certain software including drivers and documents may be available from NVIDIA. If you select a URL that directs you to http://www.nvidia.com/, you are then leaving HPE.com. Please follow the instructions on http://www.nvidia.com/ to download NVIDIA software or documentation. When downloading the NVIDIA software or documentation, you may be subject to NVIDIA terms and conditions, including licensing terms, if any, provided on its website or otherwise. HPE is not responsible for your use of any software or documents that you download from http://www.nvidia.com/, except that HPE may provide a limited warranty for NVIDIA software in accordance with the terms and conditions of your purchase of the HPE product or solution.

A list of known issues with this release is available at: https://docs.nvidia.com/networking/display/connectx6firmwarev20401000/known+issues

Prerequisites

FWPKG will work only if the firmware version flashed on the adapter is 20.27.1016 or later and iLO5 firmware version must be 2.30 or higher.

Fixes

The following issues have been fixed in version 20.40.1000:

- RDE LLDPTransmit ChassisID was occassionally not represented correctly.

Enhancements

Security Hardening Enhancements: This release contains important reliability improvements and security hardening enhancements. HPE recommends upgrading your device's firmware to this release to improve the firmware security and reliability of your device.

No New features or changes have been included in version 20.40.1000.

Supported Devices and Features

This software package contains the following firmware versions:

Mellanox InfiniBand Adapter	Firmware Version	PSID
HPE InfiniBand HDR/Ethernet 200Gb 1-port QSFP56 PCIe4 x16 MCX653105A-HDAT Adapter (P23664-B21 and P23664-H21)	20.40.1000	MT_0000000451

Mellanox Firmware Package (FWPKG) for HPE InfiniBand HDR/Ethernet 200Gb 1-port QSFP56 PCIe4 x16 OCP3 MCX653435A-HDAI Adapter : HPE part numbers P31323-B21 and P31323-H21
Version: 20.40.1000 **(Recommended)**
Filename: 20_40_1000-MCX653435A-HDA_HPE_Ax.pldm.fwpkg

Important Note!

For PLDM enabled VPI (Virtual Protocol Interconnect) adapters supporting both InfiniBand mode and Ethernet modes, every firmware version is made available in two different formats at HPE.com:

1. HPE signed PLDM Firmware Package (.FWPKG filename extension) updatable via iLO.
2. Firmware binary (.bin filename extension) updatable via mstflint utility from the Operating System.

Choose the appropriate firmware file format based on your preference and what suits your environment.

Disclaimer: Certain software including drivers and documents may be available from NVIDIA. If you select a URL that directs you to http://www.nvidia.com/, you are then leaving HPE.com. Please follow the instructions on http://www.nvidia.com/ to download NVIDIA software or documentation. When downloading the NVIDIA software or documentation, you may be subject to NVIDIA terms and conditions, including licensing terms, if any, provided on its website or otherwise. HPE is not responsible for your use of any software or documents that you download from http://www.nvidia.com/, except that HPE may provide a limited warranty for NVIDIA software in accordance with the terms and conditions of your purchase of the HPE product or solution.

A list of known issues with this release is available at: https://docs.nvidia.com/networking/display/connectx6firmwarev20401000/known+issues

Prerequisites

FWPKG will work only if the firmware version flashed on the adapter is 20.27.1016 or later and iLO5 firmware version must be 2.30 or higher.

Fixes

The following issues have been fixed in version 20.40.1000:

- RDE LLDPTransmit ChassisID was occassionally not represented correctly.

Enhancements

Security Hardening Enhancements: This release contains important reliability improvements and security hardening enhancements. HPE recommends upgrading your device's firmware to this release to improve the firmware security and reliability of your device.

No New features or changes have been included in version 20.40.1000.

Supported Devices and Features

This software package contains the following firmware versions:

Mellanox InfiniBand Adapter	Firmware Version	PSID
HPE InfiniBand HDR/Ethernet 200Gb 1-port QSFP56 PCIe4 x16 OCP3 MCX653435A-HDAI Adapter (P31323-B21 and P31323-H21)	20.40.1000	MT_0000000592

Mellanox Firmware Package (FWPKG) for HPE InfiniBand HDR/Ethernet 200Gb 2-port QSFP56 PCIe4 x16 MCX653106A-HDAT Adapter : HPE part numbers P31324-B21 and P31324-H21
Version: 20.40.1000 **(Recommended)**
Filename: 20_40_1000-MCX653106A-HDA_HPE_Ax.pldm.fwpkg

Important Note!

For PLDM enabled VPI (Virtual Protocol Interconnect) adapters supporting both InfiniBand mode and Ethernet modes, every firmware version is made available in two different formats at HPE.com:

1. HPE signed PLDM Firmware Package (.FWPKG filename extension) updatable via iLO.
2. Firmware binary (.bin filename extension) updatable via mstflint utility from the Operating System.

Choose the appropriate firmware file format based on your preference and what suits your environment.

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**
200GbE/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	**200GbE/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

A list of known issues with this release is available at: https://docs.nvidia.com/networking/display/connectx6firmwarev20401000/known+issues

Prerequisites

FWPKG will work only if the firmware version flashed on the adapter is 20.27.1016 or later and iLO5 firmware version must be 2.30 or higher.

Fixes

The following issues have been fixed in version 20.40.1000:

- RDE LLDPTransmit ChassisID was occassionally not represented correctly.

Enhancements

Security Hardening Enhancements: This release contains important reliability improvements and security hardening enhancements. HPE recommends upgrading your device's firmware to this release to improve the firmware security and reliability of your device.

No New features or changes have been included in version 20.40.1000.

Supported Devices and Features

This software package contains the following firmware versions:

Mellanox InfiniBand Adapter	Firmware Version	PSID
HPE InfiniBand HDR/Ethernet 200Gb 2-port QSFP56 PCIe4 x16 MCX653106A-HDAT Adapter(P31324-B21 and P31324-H21)	20.40.1000	MT_0000000594

Mellanox Firmware Package (FWPKG) for HPE InfiniBand HDR/Ethernet 200Gb 2-port QSFP56 PCIe4 x16 OCP3 MCX653436A-HDAI Adapter : HPE part numbers P31348-B21 and P31348-H21
Version: 20.40.1000 **(Recommended)**
Filename: 20_40_1000-MCX653436A-HDA_HPE_Ax.pldm.fwpkg

Important Note!

For PLDM enabled VPI (Virtual Protocol Interconnect) adapters supporting both InfiniBand mode and Ethernet modes, every firmware version is made available in two different formats at HPE.com:

1. HPE signed PLDM Firmware Package (.FWPKG filename extension) updatable via iLO.
2. Firmware binary (.bin filename extension) updatable via mstflint utility from the Operating System.

Choose the appropriate firmware file format based on your preference and what suits your environment.

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**
200GbE/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	**200GbE/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

Disclaimer: Certain software including drivers and documents may be available from NVIDIA. If you select a URL that directs you to http://www.nvidia.com/, you are then leaving HPE.com. Please follow the instructions on http://www.nvidia.com/ to download NVIDIA software or documentation. When downloading the NVIDIA software or documentation, you may be subject to NVIDIA terms and conditions, including licensing terms, if any, provided on its website or otherwise. HPE is not responsible for your use of any software or documents that you download from http://www.nvidia.com/, except that HPE may provide a limited warranty for NVIDIA software in accordance with the terms and conditions of your purchase of the HPE product or solution.

A list of known issues with this release is available at: https://docs.nvidia.com/networking/display/connectx6firmwarev20401000/known+issues

Prerequisites

FWPKG will work only if the firmware version flashed on the adapter is 20.27.1016 or later and iLO5 firmware version must be 2.30 or higher.

Fixes

The following issues have been fixed in version 20.40.1000:

- RDE LLDPTransmit ChassisID was occassionally not represented correctly.

Enhancements

Security Hardening Enhancements: This release contains important reliability improvements and security hardening enhancements. HPE recommends upgrading your device's firmware to this release to improve the firmware security and reliability of your device.

No New features or changes have been included in version 20.40.1000.

Supported Devices and Features

This software package contains the following firmware versions:

Mellanox InfiniBand Adapter	**Firmware Version**	**PSID**
HPE InfiniBand HDR/Ethernet 200Gb 2-port QSFP56 PCIe4 x16 OCP3 MCX653436A-HDAI Adapter (P31348-B21 and P31348-H21)	20.40.1000	MT_0000000593

Mellanox Firmware Package (FWPKG) for HPE InfiniBand HDR100/Ethernet 100Gb 1-port QSFP56 PCIe4 x16 MCX653105A-ECAT Adapter : HPE part numbers P23665-B21 and P23665-H21
Version: 20.40.1000 **(Recommended)**
Filename: 20_40_1000-MCX653105A-ECA_HPE_Ax.pldm.fwpkg

Important Note!

For PLDM enabled VPI (Virtual Protocol Interconnect) adapters supporting both InfiniBand mode and Ethernet modes, every firmware version is made available in two different formats at HPE.com:

1. HPE signed PLDM Firmware Package (.FWPKG filename extension) updatable via iLO.
2. Firmware binary (.bin filename extension) updatable via mstflint utility from the Operating System.

Choose the appropriate firmware file format based on your preference and what suits your environment.

Disclaimer: Certain software including drivers and documents may be available from NVIDIA. If you select a URL that directs you to http://www.nvidia.com/, you are then leaving HPE.com. Please follow the instructions on http://www.nvidia.com/ to download NVIDIA software or documentation. When downloading the NVIDIA software or documentation, you may be subject to NVIDIA terms and conditions, including licensing terms, if any, provided on its website or otherwise. HPE is not responsible for your use of any software or documents that you download from http://www.nvidia.com/, except that HPE may provide a limited warranty for NVIDIA software in accordance with the terms and conditions of your purchase of the HPE product or solution.

A list of known issues with this release is available at: https://docs.nvidia.com/networking/display/connectx6firmwarev20401000/known+issues

Prerequisites

FWPKG will work only if the firmware version flashed on the adapter is 20.27.1016 or later and iLO5 firmware version must be 2.30 or higher.

Fixes

The following issues have been fixed in version 20.40.1000:

- RDE LLDPTransmit ChassisID was occassionally not represented correctly.

Enhancements

Security Hardening Enhancements: This release contains important reliability improvements and security hardening enhancements. HPE recommends upgrading your device's firmware to this release to improve the firmware security and reliability of your device.

No New features or changes have been included in version 20.40.1000.

Supported Devices and Features

This software package contains the following firmware versions:

Mellanox InifiniBand Adapter	Firmware Version	PSID
HPE InfiniBand HDR100/Ethernet 100Gb 1-port QSFP56 PCIe4 x16 MCX653105A-ECAT Adapter (P23665-B21 and P23665-H21)	20.40.1000	MT_0000000452

Mellanox Firmware Package (FWPKG) for HPE InfiniBand HDR100/Ethernet 100Gb 2-port QSFP56 PCIe4 x16 MCX653106A-ECAT Adapter : HPE part numbers P23666-B21 and P23666-H21
Version: 20.40.1000 **(Recommended)**
Filename: 20_40_1000-MCX653106A-ECA_HPE_Ax.pldm.fwpkg

Important Note!

For PLDM enabled VPI (Virtual Protocol Interconnect) adapters supporting both InfiniBand mode and Ethernet modes, every firmware version is made available in two different formats at HPE.com:

1. HPE signed PLDM Firmware Package (.FWPKG filename extension) updatable via iLO.
2. Firmware binary (.bin filename extension) updatable via mstflint utility from the Operating System.

Choose the appropriate firmware file format based on your preference and what suits your environment.

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

Disclaimer: Certain software including drivers and documents may be available from NVIDIA. If you select a URL that directs you to http://www.nvidia.com/, you are then leaving HPE.com. Please follow the instructions on http://www.nvidia.com/ to download NVIDIA software or documentation. When downloading the NVIDIA software or documentation, you may be subject to NVIDIA terms

and conditions, including licensing terms, if any, provided on its website or otherwise. HPE is not responsible for your use of any software or documents that you download from http://www.nvidia.com/, except that HPE may provide a limited warranty for NVIDIA software in accordance with the terms and conditions of your purchase of the HPE product or solution.

A list of known issues with this release is available at: https://docs.nvidia.com/networking/display/connectx6firmwarev20401000/known+issues

Prerequisites

FWPKG will work only if the firmware version flashed on the adapter is 20.27.1016 or later and iLO5 firmware version must be 2.30 or higher.

Fixes

The following issues have been fixed in version 20.40.1000:

- RDE LLDPTransmit ChassisID was occassionally not represented correctly.

Enhancements

Security Hardening Enhancements: This release contains important reliability improvements and security hardening enhancements. HPE recommends upgrading your device's firmware to this release to improve the firmware security and reliability of your device.

No New features or changes have been included in version 20.40.1000.

Supported Devices and Features

This software package contains the following firmware versions:

Mellanox InfiniBand Adapter	Firmware Version	PSID
HPE InfiniBand HDR100/Ethernet 100Gb 2-port QSFP56 PCIe4 x16 MCX653106A-ECAT Adapter (P23666-B21 and P23666-H21)	20.40.1000	MT_0000000453

Mellanox Firmware Package(FWPKG) for HPE NV60025M Ethernet 10/25Gb 2-port Secure Network Adapter
Version: 26.38.1002 **(Recommended)**
Filename: 26_38_1002-S2A69-63001_Ax_header.pldm.fwpkg

Important Note!

Known Issues with firmware version 26.38.1002:

- Multi-APP QoS is not supported when LAG is configured.
- When Emulated PCIe Switch is enabled, and more than 8 PFs are enabled, the OS boot process might halt.
- When Emulated PCIe Switch is enabled, and the OS does resource reallocation, the OS boot process might halt.
- Unable to complete migration when virtio device is in high traffic load (20/20 MPPS) as although vDPA hardware offload solution can support higher speed than the software solution, it needs to enable QEMU auto-converge to complete migration.
- Using the Eye-Opening tool might cause degradation in the link speed or link down events.
- Sub 1sec firmware update (fast reset flow) is not supported when updating from previous releases to the current one. Doing so may cause network disconnection events.
- On systems with high PCIe latency (2us or above), lower bandwidth may be experienced. .

Prerequisites

FWPKG will work only if the firmware version flashed on the adapter is 22.27.1016 or later and iLO5 firmware version must be 2.30 or higher.

Enhancements

New features and changes included in version 26.38.1002:

- Enabled 200Gb/s out-of-the-box throughput on crypto capable devices.
  Note: If any crypto offloads is in use, 200Gb/s throughput can be achieved only after the next firmware reset
- Added support for VF migration. The hypervisor can now suspend its VF, meaning from that point the VF cannot perform action such as send/receive traffic or run any command. In this firmware version only the suspend resume mode is

supported (on the same VM).
- Added a new MAD of class SMP that has the attributes hierarchy_Info as defined in the IB Specification and is used to query the hierarchy information stored on the node and the physical port.
- Added pci_rescan_needed field to the MFRL access register to indicate whether a PCI rescan is needed based on the NV configurations issued by the software.
  Note: If the Keep Link Up NV configuration is changed, phyless reset will be blocked.
- Added Precision Time Protocol (PTP) support.
  In this version, the support includes:
  16 PTP SQs only
  only 2 ports
  only RT clock mode
  In this version, the following are not supported:
  PTP packet drop
  PTP SQ on VF
  Note: All PTP SQs must be closed before operating LFWP (life fw patch).
- Added support for HW Steering objects dump via resource dump interface.
  This support includes: STC, RTC, STE, modify argument, and modify pattern.
- Added support for VF migration.
- Added a new register (vhca_icm_ctrl access_reg) to enable querying and limiting the ICM pages in use.
- Added support for creating a steering definer with a dword selector using create_match_definer_object and the "SELECT" format.
- Enhanced the XRQ QP error information provided to the user in case QP goes into an error state. In such case, QUERY_QP will provide information on the syndrome type and which side caused the error.
- [Beta] Added HW Steering support for the following:
  set, add and copy inline STC action
  set and copy actions for several fields using modify_pattern object and inline stc modify action
  FDB mode in HW steering using FDB_RX and FDB_TX flow table types
  ASO flow meter action via STC
  flow counter query using ASO WQE
  allocation of large bulks for the objects: STE, ASO flow meter and modify argument
  jumbo match RTC
  count action in STC
- Added support for holdover mode to comply to SyncE specifications (EEC compliance) to limit the maximum phase transient response upon link loss.
- Added support for noise filtering to comply to the SyncE specifications requirements.
- Optimized the performance of vDPA virtio including: throughput, QoS, and accuracy of min/max bandwidth when virtio works with the QoS settings.
- The new vDPA virtio-net Full Emulation capability reduces the switchover time of creating a virtq from scratch during live migration, by creating the virtq beforehand on the target server.
  When swithover happens, the pre-created virtq will be used and modified with necessary parameters.
- Updated the ibstat status reported when the phy link is down. Now QUERY_VPORT_STATE.max_tx_speed of UPLINK will not be reported as 0 anymore.
- Replaced the deprecated NetworkPort schema with Port schema in NIC RDE implementation.
- Enabled the option to modify the ip_ecn field in the packet header in firmware steering.
- Added support for advanced ZTR_RTTCC algorithm based on the Programmable CC platform to achieve better congestion control without dependency on the switch ECN marking.
- DIM is used to tune moderation parameter dynamically for vDPA using an mlxreg command.
  To disable this capability, run:
  mlxreg -d /dev/mst/mt41686_pciconf0 --reg_id 0xc00d --reg_len 0x8 -s "0x4.1:1=0x0"
- Modified the TX or RX cache invalidation behavior. TX or RX cache invalidation now does not occur automatically but only when the software performs the sync operation using the using sync_steering command.
- Modified the maximum bulk size per single allocation from "log_table_size - log_num_unisizes", to allocate any range size, to remove limitations that HWS objects such as counters and modify arguments might encounter.
- Added support for creating a dynamic flex parser on untrusted function, and changed the flex parser cap for untrusted function to the following:
  maximum flex parser node = 2
  maximum dw sample = 4
- Added support for SNAPI (comm-channel) connection while running on raw ETH link.
- Crypto features can be in either wrapped or unwrapped mode. Meaning, the key can be wrapped or in plaintext when running the CREATE_DEK PRM command.
  To comply with the requirements specified in FIPS publication, all the created DEKs must be wrapped.
  This feature adds new NV_CONFIG per device to control this mode, and enables the user to change all the crypto features to wrapped or cleartext.
- [Beta] A new capability that enables the software to directly access ICM and write/modify the DEK objects. Such change improves the DEK object update rate by re-using DEK object instead of creating a new one.
  In addition, added the following:
  New for DEK object: bulk allocation, modify_dek cmd, and new mode - sw_wrapped.
  New general object INT_KEK

Supported Devices and Features

HPE Part Number	Mellanox Ethernet Only Adapters	PSID
P46603-B21	HPE NV60025M Ethernet 10/25Gb 2-port Secure Network Adapter	HPE0000000062

Mellanox Firmware Package(FWPKG) for HPE NV60100M 100Gb 2-port Storage Offload Adapter
Version: 22.38.1002 **(Recommended)**
Filename: 22_38_1002-R8M41-63001_Ax_header.pldm.fwpkg

Important Note!

Known Issues with firmware version 22.38.1002:

- Multi-APP QoS is not supported when LAG is configured.
- When Emulated PCIe Switch is enabled, and more than 8 PFs are enabled, the OS boot process might halt.
- When Emulated PCIe Switch is enabled, and the OS does resource reallocation, the OS boot process might halt.
- Unable to complete migration when virtio device is in high traffic load (20/20 MPPS) as although vDPA hardware offload solution can support higher speed than the software solution, it needs to enable QEMU auto-converge to complete migration.
- Using the Eye-Opening tool might cause degradation in the link speed or link down events.
- Sub 1sec firmware update (fast reset flow) is not supported when updating from previous releases to the current one. Doing so may cause network disconnection events.
- On systems with high PCIe latency (2us or above), lower bandwidth may be experienced. .

Prerequisites

FWPKG will work only if the firmware version flashed on the adapter is 22.27.1016 or later and iLO5 firmware version must be 2.30 or higher.

Enhancements

New features and changes included in version 22.38.1002:

- Enabled 200Gb/s out-of-the-box throughput on crypto capable devices.
  Note: If any crypto offloads is in use, 200Gb/s throughput can be achieved only after the next firmware reset
- Added support for VF migration. The hypervisor can now suspend its VF, meaning from that point the VF cannot perform action such as send/receive traffic or run any command. In this firmware version only the suspend resume mode is supported (on the same VM).
- Added a new MAD of class SMP that has the attributes hierarchy_Info as defined in the IB Specification and is used to query the hierarchy information stored on the node and the physical port.
- Added pci_rescan_needed field to the MFRL access register to indicate whether a PCI rescan is needed based on the NV configurations issued by the software.
  Note: If the Keep Link Up NV configuration is changed, phyless reset will be blocked.
- Added Precision Time Protocol (PTP) support.
  In this version, the support includes:
  16 PTP SQs only
  only 2 ports
  only RT clock mode
  In this version, the following are not supported:
  PTP packet drop
  PTP SQ on VF
  Note: All PTP SQs must be closed before operating LFWP (life fw patch).
- Added support for HW Steering objects dump via resource dump interface.
  This support includes: STC, RTC, STE, modify argument, and modify pattern.
- Added support for VF migration.
- Added a new register (vhca_icm_ctrl access_reg) to enable querying and limiting the ICM pages in use.
- Added support for creating a steering definer with a dword selector using create_match_definer_object and the "SELECT" format.
- Enhanced the XRQ QP error information provided to the user in case QP goes into an error state. In such case, QUERY_QP will provide information on the syndrome type and which side caused the error.
- [Beta] Added HW Steering support for the following:
  set, add and copy inline STC action
  set and copy actions for several fields using modify_pattern object and inline stc modify action
  FDB mode in HW steering using FDB_RX and FDB_TX flow table types
  ASO flow meter action via STC
  flow counter query using ASO WQE
  allocation of large bulks for the objects: STE, ASO flow meter and modify argument
  jumbo match RTC
  count action in STC
- Added support for holdover mode to comply to SyncE specifications (EEC compliance) to limit the maximum phase transient response upon link loss.
- Added support for noise filtering to comply to the SyncE specifications requirements.

Optimized the performance of vDPA virtio including: throughput, QoS, and accuracy of min/max bandwidth when virtio works with the QoS settings.
- The new vDPA virtio-net Full Emulation capability reduces the switchover time of creating a virtq from scratch during live migration, by creating the virtq beforehand on the target server.
  When swithover happens, the pre-created virtq will be used and modified with necessary parameters.
- Updated the ibstat status reported when the phy link is down. Now QUERY_VPORT_STATE.max_tx_speed of UPLINK will not be reported as 0 anymore.
- Replaced the deprecated NetworkPort schema with Port schema in NIC RDE implementation.
- Enabled the option to modify the ip_ecn field in the packet header in firmware steering.
- Added support for advanced ZTR_RTTCC algorithm based on the Programmable CC platform to achieve better congestion control without dependency on the switch ECN marking.
- DIM is used to tune moderation parameter dynamically for vDPA using an mlxreg command.
  To disable this capability, run:
  mlxreg -d /dev/mst/mt41686_pciconf0 --reg_id 0xc00d --reg_len 0x8 -s "0x4.1:1=0x0"
- Modified the TX or RX cache invalidation behavior. TX or RX cache invalidation now does not occur automatically but only when the software performs the sync operation using the using sync_steering command.
- Modified the maximum bulk size per single allocation from "log_table_size - log_num_unisizes", to allocate any range size, to remove limitations that HWS objects such as counters and modify arguments might encounter.
- Added support for creating a dynamic flex parser on untrusted function, and changed the flex parser cap for untrusted function to the following:
  maximum flex parser node = 2
  maximum dw sample = 4
- Added support for SNAPI (comm-channel) connection while running on raw ETH link.
- Crypto features can be in either wrapped or unwrapped mode. Meaning, the key can be wrapped or in plaintext when running the CREATE_DEK PRM command.
  To comply with the requirements specified in FIPS publication, all the created DEKs must be wrapped.
  This feature adds new NV_CONFIG per device to control this mode, and enables the user to change all the crypto features to wrapped or cleartext.
- [Beta] A new capability that enables the software to directly access ICM and write/modify the DEK objects. Such change improves the DEK object update rate by re-using DEK object instead of creating a new one.
  In addition, added the following:
  New for DEK object: bulk allocation, modify_dek cmd, and new mode - sw_wrapped.
  New general object INT_KEK

Supported Devices and Features

HPE Part Number	Mellanox Ethernet Only Adapters	PSID
P46603-B21	HPE NV60100M 100Gb 2-port Storage Offload Adapter	HPE0000000062

Online Firmware Upgrade Utility (ESXi 8.0) for HPE Ethernet 10Gb 2-port 548SFP+ Adapter
Version: 1.0.0 **(Recommended)**
Filename: CP053859.compsig; CP053859.zip

Prerequisites

Use iLO5 firmware version 2.30 or higher with ConnectX4-Lx firmware version 14.32.1010. 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 14.32.1010:

- Firmware got into an unresponsive state and caused unexpected behavior when connecting an optical transceiver that support RxLOS and the remote side port was down.
- The system could not create more than 128K QPs.
- On rare occasions, the system got into an unresponsive state when a peer port went down while using an Optical module.
- Packet Pacing rate was used if asymmetric VFs was enabled.
- Incorrect RNR timeout when trying to set it during the rts2rts_qp transition.
- Issue with RSS on IPSec flows in ConnectX-4 Lx led to performance degradation. In this scenario, the SPI optimization caused packets from a given host to hash to the same CPU core. The fix was to ignore SPI optimization according to l4_type in ConnectX-4 Lx adapter cards.
- The GetInventory NC-SI command reported leading 0xf in firmware version when it started with 0.

Enhancements

Firmware for the following device has been updated to 14.32.1010:

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

New features and changes included in version 14.32.1010:

- Added 3 new assert filters (Health buffer, NVlog, FW trace). The assert will be exposed now if its severity level is equal to or above the new filter.
- Enabled Rate Limit per VM instead of VM-TC. This capability is implemented by adding support to a new Scheduling element type: rate limit elements that will connect to the rate_limit and will share its rate limit.
- Added support for asymmetrical VFs per PF. To enable it:PF_NUM_OF_VF_VALID must be true, and PF_NUM_OF_VF to a non-zero value.
- Limited the external loopback speed to the used module's capabilities.
- Improved linkup time when using the fast linkup capability.
- Added support for the slow_restart and slow_restart_idle parameters to enable Zero Touch RoCE capability.

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 8.0) for HPE Mellanox Ethernet only adapters
Version: 1.0.3 **(Recommended)**
Filename: CP057775.compsig; CP057775.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.

Prerequisites

Use iLO5 firmware version 2.30 or higher with ConnectX4-Lx/ConnectX5 firmware version 14.32.1010/16.32.1010 (or later) respectively. 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 14.32.1010:

- Firmware got into an unresponsive state and caused unexpected behavior when connecting an optical transceiver that support RxLOS and the remote side port was down.
- The system could not create more than 128K QPs.
- On rare occasions, the system got into an unresponsive state when a peer port went down while using an Optical module.
- Packet Pacing rate was used if asymmetric VFs was enabled.
- Incorrect RNR timeout when trying to set it during the rts2rts_qp transition.
- Issue with RSS on IPSec flows in ConnectX-4 Lx led to performance degradation. In this scenario, the SPI optimization caused packets from a given host to hash to the same CPU core. The fix was to ignore SPI optimization according to l4_type in ConnectX-4 Lx adapter cards.
- The GetInventory NC-SI command reported leading 0xf in firmware version when it started with 0.

The following issues have been fixed in version 16.35.3006:

- Packet loss that occurred when restarting the transmit.
- An issue that prevented RoCE malformed packets (UDP packet with dest_port equal to RoCE well known udp_dport (0x4791)) from being counted on the vport_counter when the function disables RoCE (through MODIFY_NIC_VPORT_CONTEXT command).
- A memory leakage that occurred when closing connected QPs (Type RC/UC/XRC/DC).
- Added a missing VLAN strip.

Enhancements

Firmware for the following devices has been updated to 14.32.1010:

- 817749-B21 (HPE Ethernet 25Gb 2-port 640FLR-SFP28 Adapter)
- 817753-B21 (HPE Ethernet 25Gb 2-port 640SFP28 Adapter)

Firmware for the following device has been updated to 16.35.3006:

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

New features and changes included in version 14.32.1010:

- Added 3 new assert filters (Health buffer, NVlog, FW trace). The assert will be exposed now if its severity level is equal to or above the new filter.
- Enabled Rate Limit per VM instead of VM-TC. This capability is implemented by adding support to a new Scheduling element type: rate limit elements that will connect to the rate_limit and will share its rate limit.
- Added support for asymmetrical VFs per PF. To enable it:PF_NUM_OF_VF_VALID must be true, and PF_NUM_OF_VF to a non-zero value.
- Limited the external loopback speed to the used module's capabilities.
- Improved linkup time when using the fast linkup capability.
- Added support for the slow_restart and slow_restart_idle parameters to enable Zero Touch RoCE capability.

New features and changes included in version 16.35.3006:

- Enabled ACS for single port cards.
- Added vPort counters after creating the LAG demux table to count kernel packets reaching all the PFs participating in the LAG.

Supported Devices and Features

HPE Part Number	Mellanox Ethernet Only Adapters	PSID
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 8.0) for HPE Mellanox VPI (Ethernet and Infiniband mode) ConnectX4 and ConnectX5 devices on VMware ESXi 8.0
Version: 1.0.2 **(Recommended)**
Filename: CP056758.compsig; CP056758.zip

Fixes

The following issues have been fixed in version 12.28.2006:

- Fixes an issue that caused the DCR to be destroyed before the retry option managed to work when the retry timeout is too big. In this case the DCR' time-to-live was increased, and the maximum retry timeout was decreased.
- Increased PHY power consumption limit to 1.5w.
- Fixed an issue that caused PortCounters.PortRcvErr / PPCNT.infiniband_counters.PortRcvErr not to report port icrc errors.

The following issues have been fixed in version 16.35.3006:

- Packet loss that occurred when restarting the transmit.
- An issue that prevented RoCE malformed packets (UDP packet with dest_port equal to RoCE well known udp_dport (0x4791)) from being counted on the vport_counter when the function disables RoCE (through MODIFY_NIC_VPORT_CONTEXT command).
- A memory leakage that occurred when closing connected QPs (Type RC/UC/XRC/DC).
- Added a missing VLAN strip.

Enhancements

Firmware for the following devices has been updated to 12.28.2006:

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

Firmware for the following devices has been updated to 16.35.3006:

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

Important : Security Hardening Enhancements - This release contains important reliability improvements and security hardening enhancements. HPE recommends upgrading your device firmware to this version to improve the firmware security and reliability of your device.

New Features and changes included in version 12.28.2006:

- Increased the maximum XRQ number to 512.

New features and changes included in version 16.35.3006:

- Enabled ACS for single port cards.
- Added vPort counters after creating the LAG demux table to count kernel packets reaching all the PFs participating in the LAG.

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 8.0) for HPE Mellanox VPI (Ethernet and Infiniband mode) devices on VMware ESXi 8.0
Version: 1.0.0 **(Recommended)**
Filename: CP052070.compsig; CP052070.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 0xffffff).
- 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:

HPE Part Number	Device Name	PSID
764282-B21	HPE InfiniBand QDR/Ethernet 10Gb 2-port 544+M Adapter	HPE_1350110023
764283-B21	HPE InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+M Adapter	HPE_1360110017
764284-B21	HPE InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+QSFP Adapter	HPE_1370110017

764285-B21	HPE InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+FLR-QSFP Adapter	HPE_1380110017
764286-B21	HPE InfiniBand QDR/Ethernet 10Gb 2-port 544+FLR-QSFP Adapter	HPE_1390110023

Online Firmware Upgrade Utility (ESXi 8.0) for Mellanox Open Ethernet cards
Version: 1.0.3 **(Recommended)**
Filename: CP057779.compsig; CP057779.zip

Important 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-Lx/ConnectX5 firmware version 14.32.1010/16.32.1010 respectively. 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 14.32.1010:

- Firmware got into an unresponsive state and caused unexpected behavior when connecting an optical transceiver that support RxLOS and the remote side port was down.
- The system could not create more than 128K QPs.
- On rare occasions, the system got into an unresponsive state when a peer port went down while using an Optical module.
- Packet Pacing rate was used if asymmetric VFs was enabled.
- Incorrect RNR timeout when trying to set it during the rts2rts_qp transition.
- Issue with RSS on IPSec flows in ConnectX-4 Lx led to performance degradation. In this scenario, the SPI optimization caused packets from a given host to hash to the same CPU core. The fix was to ignore SPI optimization according to l4_type in ConnectX-4 Lx adapter cards.
- The GetInventory NC-SI command reported leading 0xf in firmware version when it started with 0.

The following issues have been fixed in version 16.35.3006:

- Packet loss that occurred when restarting the transmit.
- An issue that prevented RoCE malformed packets (UDP packet with dest_port equal to RoCE well known udp_dport (0x4791)) from being counted on the vport_counter when the function disables RoCE (through MODIFY_NIC_VPORT_CONTEXT command).
- A memory leakage that occurred when closing connected QPs (Type RC/UC/XRC/DC).
- Added a missing VLAN strip.

Enhancements

Firmware for the following devices has been updated to 14.32.1010:

- 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 device has been updated to 16.35.3006:

- P21927-B21 (HPE Ethernet 100Gb 2-Port QSFP28 MCX516A-CCHT Adapter)

New features and changes included in version 14.32.1010:

- Added 3 new assert filters (Health buffer, NVlog, FW trace). The assert will be exposed now if its severity level is equal to or above the new filter.
- Enabled Rate Limit per VM instead of VM-TC. This capability is implemented by adding support to a new Scheduling element type: rate limit elements that will connect to the rate_limit and will share its rate limit.
- Added support for asymmetrical VFs per PF. To enable it:PF_NUM_OF_VF_VALID must be true, and PF_NUM_OF_VF to a non-zero value.
- Limited the external loopback speed to the used module's capabilities.
- Improved linkup time when using the fast linkup capability.
- Added support for the slow_restart and slow_restart_idle parameters to enable Zero Touch RoCE capability.

New features and changes included in version 16.35.3006:

- Enabled ACS for single port cards.

Added vPort counters after creating the LAG demux table to count kernel packets reaching all the PFs participating in the LAG.

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/25Gb 2-port SFP28 MCX4621A-ACAB OCP3 Adapter	MT_0000000238
P21927-B21	HPE Ethernet 100Gb 2-port QSFP28 MCX516A-CCHT Adapter	MT_0000000417

Firmware - Storage Controller Top

Firmware Package - HPE Smart Array P408i-p, P408e-p, P408i-a, P408i-c, E208i-p, E208e-p, E208i-c, E208i-a, P408e-m, P204i-c, P416ie-m and P816i-a SR Gen10 and Gen11 controllers
Version: 6.52 **(Recommended)**
Filename: HPE_SR_Gen10_6.52_A.fwpkg

Fixes

- Fixed issues with the SED drive.
- Fixed issues with the spare drive.
- Fixed an issue with the SmartCache logical drive.
- Fixed issues with expander firmware upgrade.
- Fixed issues with RBOD devices.
- Fixed a potential controller lockup issue while deleting a logical drive configuration on a controller.
- Resolved an issue by allowing MCTP re-discovery exclusively during the first Bus Master Enable set.
- Fixed UEFI HII unreadable characters in Chinese language.
- Fixed an issue where WriteCacheProtected alert is sometimes not generated.

Enhancements

- Added support to save controller logs in host memory in the event of a system crash.
- Added support for remote-managed SED rekey.
- Added support for Configurable Spindown Spares policy.
- Added support for the permanent disablement of unused IOBAR support in PCIe configuration space.
- Enhance Redfish interfaces:
  - support DELETE for a Volume resource which is not the last created on a given array.
  - support DELETE for the last remaining Volume on an array which has SED encryption enabled.
  - support #Storage.ResetToDefaults with ResetType = ResetAll when encrypted volumes are present.
  - support AutoVolumeCreate property in Redfish Storage resource
  - support Links.Batteries property in Redfish StorageController resource

---

Firmware Package - HPE Gen11 Boot Controller NS204i-u, NS204i-d and HPE Gen10 Plus Boot Controller NS204i-p, NS204i-d, NS204i-t, NS204i-r
Version: 1.2.14.1013 **(Recommended)**
Filename: HPE_NS204i_Gen10P_Gen11_1.2.14.1013_A.fwpkg

Important Note!

Current firmware has to be 1.0.14.1063 or later in order to enable PLDM firmware update functionality for the controller. Please find the smart component versions of 1.0.14.1063 in below link:

- Windows: https://www.hpe.com/global/swpublishing/MTX-be195b2891724ec8bb72c8bb2
- Linux: https://www.hpe.com/global/swpublishing/MTX-269e14d0e2524277bf699f433
- Vmware: https://www.hpe.com/global/swpublishing/MTX-1ffaca997cf248cd9f832a04c6

Prerequisites

- iLO 6 version 1.10 or later is required for Gen11 servers.
- iLO 5 version 2.81 or later is required for Gen10/Gen10 Plus servers

Fixes

- Fixed an issue that iLO reports NS204i PLDM firmware update failure, but the firmware update is actually successful and will be activated in next reboot
- Fixed an issue that the M.2 attached are listed in iLO Device Inventory
- Corrected the drive state of performing Storage.ResetToDefaults with ResetAll type
- Allowed empty JSON payload for SecureErase and corrected the returned status when the previous one is either in process or

completed.

Enhancements

- Add @Redfish.AllowableValues, @Redfish.AllowablePattern, @Redfish.AllowableNumbers and @Redfish.WriteableProperties for Redfish Annotations
- Add StorageController.Links, Drive.SlotCapableProtocols and Storage.AutoVolumeCreate for Redfish GET
- Add StorageController.ControllerRates and Volume.DisplayName for Redfish PATCH

Firmware Package - HPE SR932i-p Gen10 Plus /SR416i-a Gen10 Plus/SR932i-p Gen11/SR416ie-m Gen11 Controllers
Version: 03.01.23.072 **(Recommended)**
Filename: HPE_SR416_SR932_Gen10P_Gen11_03.01.23.072_A.fwpkg

Fixes

- Fixed issues related to spare drive functionality.
- Fixed issues pertaining to Self-Encrypting Drive (SED) functionality.
- Fixed an issue where rebuild was being reiterated continuously and not progressing.
- Fixed controller detection issues during system boot, including rare cases that could lead to PSOD or RSOD errors.
- Fixed an issue where the SR932i-p Gen11 controller was not assigned an EID.
- Fixed an issue where rebuild was being reiterated continuously and not progressing.
- Fixed an issue where Redfish events of battery and WriteCache do not meet requirements.
- Fixed an issue where firmware incorrectly reported unrecoverable media errors.
- Fixed an issue where the surface scan progress status is displayed as "In progress" even after disabling the surface scan on the controller.
- Fixed an issue where rebuild was being reiterated continuously and not progressing.
- Fixed an issue related to the failure of the clear controller configuration command.
- Fixed an issue where an Uncorrectable error PSOD observed after power on.
- Fixed an issue where the Unique ID of different SATA disks is the same in Windows.
- Fixed an issue of power surge when too many SATA drives are spinning up simultaneously.
- Fixed issues where logical drives were lost after a controller reset to factory defaults, especially when the 'preserve logical drive' option was enabled, and after an abrupt reboot where the controller reset to factory defaults, causing RAID loss.
- Fixed migrating a SmartCache when destination controller has existing logical drive.
- Fixed inaccuracies in SES enclosure behavior during hot-adding and hot-removing procedures.
- Fixed an issue where the controller was providing incorrect mode page information regarding the Write Cache attribute of NVMe drives.
- Fixed an issue causing system freezes during boot after enabling Secured-Core (DMAr) in RBSU.
- Fixed an issue where the BatteryMissing event was not being sent when the battery was removed prior to boot.
- Fixed an issue where a DriveOffline Redfish alert is not sent when a Drive resource initiated a sanitize operation.
- Fixed an issue where the controller's attempt to update an unflashable UBM resulted in an error report.
- Fixed an issue where an unflashable SMP PSOC (System Management Processor Programmable System-on-Chip) device was incorrectly appearing in the Type 5 downstream devices.
- Fixed an issue where driver health error messages were not displayed when the system language was changed to a non-English language.
- Fixed an issue of incorrectly reporting the WriteCachePolicy for a Volume resource as "ProtectedWriteBack" when the cache was temporarily disabled.
- Correct Redfish properties when backup power source is removed.
- Fixed an issue where the controller failed to report storage information in the absence of physical drives.
- Fixed an issue where an unexpected 'BatteryCharging' event was reported when no battery was present.

Enhancements

- Added support for improving secure erase time for disks supporting the WRITE SAME command.
- Added support for switching persistent event log policy without clearing the existing event logs.
- Added support for Remote Key Management of Managed SED.
- Added support for 256 bytes Key Management Service (KMS) key identifier.
- Added support for reporting surface scan metrics for host management tools.
- Added support to allow re-enabling logical drive with rebuild option.
- Introduce an HII option labeled 'Configure Controller UEFI Driver Health Reporting' within the 'Configure Controller Settings' menu to provide the capability to enable or disable the reporting of configuration errors and driver health.
- Introduce an HII option labeled 'Controller Password State' within the CBE (Controller-Based Encryption) settings, enabling the actions to unset, temporarily suspend, and resume the controller password.
- Updated the Redfish resource to align with the DMTF 2022.2 schema bundle, including the incorporation of Redfish annotations.
- Adjusted the severity for Redfish Volume Status.Health state and DriveOffline alert for Foreign SED.
- Create Redfish Volumes with a RAIDType set to 'None' for HBA (Host Bus Adapter) drives.

Online Firmware Flash for ESXi - HPE Gen10 Plus Boot Controller NS204i-p, NS204i-d, NS204i-t, NS204i-r
Version: 1.0.14.1063 **(Recommended)**
Filename: CP056151.compsig; CP056151.zip

Important Note!

- VMware **7.0u1 is** supported by HPE NS204i-p, NS204i-d, NS204i-t and NS204i-r Gen10+ Boot Controller
- **VMware 7.0 is NOT supported by HPE NS204i-p, NS204i-d, NS204i-t and NS204i-r Gen10+ Boot Controller**
- **This version is the minimum required version for Gen10 Plus device to upgrade to latest FW**
- **You can get Firmware Package version 1.2.14.1004 or latest FW version from https://www.hpe.com/global/swpublishing/MTX-318c8e8298704d8bb4f991eb4d and update it via iLO without any OS dependency.**

Fixes

Fix known issue on v1055 regarding RDE dictionary broken which will cause unexpected FW upgrading error.

Online ROM Flash Component for VMware ESXi - HPE 12Gb/s SAS Expander Firmware for HPE Smart Array Controllers and HPE HBA Controllers
Version: 5.15 (B) **(Recommended)**
Filename: CP057012.compsig; CP057012.zip

Important Note!

- **Do NOT downgrade FW to previous version if your current expander is 5.10; please upgrade to 5.15 immediately.**

Enhancements

- Support HPE ProLiant DL180 Gen10 Server

Online ROM Flash Component for VMware ESXi - HPE Smart Array P408i-p, P408e-p, P408i-a, E208i-p, E208e-p, E208i-a, P816i-a SR Gen10
Version: 5.61 (D) **(Recommended)**
Filename: CP057475.compsig; CP057475.zip

Enhancements

Support Gen10, Gen10 Plus and Gen11 servers

Online ROM Flash Component for VMware ESXi - HPE Smart Array P408i-p, P408e-p, P408i-a, E208i-p, E208e-p, E208i-a, P816i-a SR Gen10
Version: 6.52 **(Recommended)**
Filename: CP058431.compsig; CP058431.zip

Fixes

- Fixed issues with the SED drive.
- Fixed issues with the spare drive.
- Fixed an issue with the SmartCache logical drive.
- Fixed issues with expander firmware upgrade.
- Fixed issues with RBOD devices.
- Fixed a potential controller lockup issue while deleting a logical drive configuration on a controller.
- Resolved an issue by allowing MCTP re-discovery exclusively during the first Bus Master Enable set.
- Fixed UEFI HII unreadable characters in Chinese language.
- Fixed an issue where WriteCacheProtected alert is sometimes not generated.

Enhancements

- Added support to save controller logs in host memory in the event of a system crash.
- Added support for remote-managed SED rekey.
- Added support for Configurable Spindown Spares policy.
- Added support for the permanent disablement of unused IOBAR support in PCIe configuration space.
- Enhance Redfish interfaces:
  - support DELETE for a Volume resource which is not the last created on a given array.
  - support DELETE for the last remaining Volume on an array which has SED encryption enabled.
  - support #Storage.ResetToDefaults with ResetType = ResetAll when encrypted volumes are present.
  - support AutoVolumeCreate property in Redfish Storage resource
  - support Links.Batteries property in Redfish StorageController resource

Firmware - Storage Fibre Channel

Top

HPE Firmware Flash for Emulex Fibre Channel Host Bus Adapters for VMware vSphere 8.0
Version: 2023.10.01 **(Recommended)**
Filename: CP058598.compsig; CP058598.zip

Important Note!

Release notes:

Broadcom Release notes

This Firmware package contains following firmware versions:

Adapter	Speed	Universal Boot Image	Firmware	UEFI	Boot Bios
HPE SN1200E 16Gb Dual Port Fibre Channel Host Bus Adapter	16Gb	14.2.589.21	14.2.589.21	14.2.589.16	14.2.566.0
HPE SN1200E 16Gb Single Port Fibre Channel Host Bus Adapter	16Gb	14.2.589.21	14.2.589.21	14.2.589.16	14.2.566.0
HPE SN1600E 32Gb Dual Port Fibre Channel Host Bus Adapter	32Gb	14.2.589.21	14.2.589.21	14.2.589.16	14.2.566.0
HPE SN1600E 32Gb Single Port Fibre Channel Host Bus Adapter	32Gb	14.2.589.21	14.2.589.21	14.2.589.16	14.2.566.0
HPE SN1610E 32Gb Single Port Fibre Channel Host Bus Adapter	32Gb	14.2.589.19	14.2.589.19	14.2.589.16	14.2.566.0
HPE SN1610E 32Gb Dual Port Fibre Channel Host Bus Adapter	32Gb	14.2.589.19	14.2.589.19	14.2.589.16	14.2.566.0
HPE SN1700E 64Gb Single Port Fibre Channel Host Bus Adapter	64Gb	14.2.589.19	14.2.589.19	14.2.589.16	14.2.566.0
HPE SN1700E 64Gb Dual Port Fibre Channel Host Bus Adapter	64Gb	14.2.589.19	14.2.589.19	14.2.589.16	14.2.566.0

Prerequisites

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

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

Enhancements

This Firmware package contains following firmware versions:

Adapter	Speed	Universal Boot Image	Firmware	UEFI	Boot Bios
HPE SN1200E 16Gb Dual Port Fibre Channel Host Bus Adapter	16Gb	14.2.589.21	14.2.589.21	14.2.589.16	14.2.566.0
HPE SN1200E 16Gb Single Port Fibre Channel Host Bus Adapter	16Gb	14.2.589.21	14.2.589.21	14.2.589.16	14.2.566.0
HPE SN1600E 32Gb Dual Port Fibre Channel Host Bus Adapter	32Gb	14.2.589.21	14.2.589.21	14.2.589.16	14.2.566.0
HPE SN1600E 32Gb Single Port Fibre Channel Host Bus Adapter	32Gb	14.2.589.21	14.2.589.21	14.2.589.16	14.2.566.0
HPE SN1610E 32Gb Single Port Fibre Channel Host Bus Adapter	32Gb	14.2.589.19	14.2.589.19	14.2.589.16	14.2.566.0
HPE SN1610E 32Gb Dual Port Fibre Channel Host Bus Adapter	32Gb	14.2.589.19	14.2.589.19	14.2.589.16	14.2.566.0
HPE SN1700E 64Gb Single Port Fibre Channel Host Bus Adapter	64Gb	14.2.589.19	14.2.589.19	14.2.589.16	14.2.566.0
HPE SN1700E 64Gb Dual Port Fibre Channel Host Bus Adapter	64Gb	14.2.589.19	14.2.589.19	14.2.589.16	14.2.566.0

Supported Devices and Features

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

16Gb FC Adapter:

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

64Gb FC Adapter:

- HPE SN1700E 64Gb Dual Port Fibre Channel Host Bus Adapter
- HPE SN1700E 64Gb Single Port Fibre Channel Host Bus Adapter

---

HPE Firmware Flash for QLogic Fibre Channel Host Bus Adapters for VMware vSphere 8.0
Version: 2023.10.01 **(Recommended)**
Filename: CP058496.compsig; CP058496.zip

Important Note!

Release Notes:
HPE QLogic Adapters Release Notes

This Firmware package contains following firmware versions:

Adapter	Speed	MBI	Firmware	UEFI	Boot Bios
HPE SN1100Q 16GB Dual Port PCIe Fibre Channel Host Bus Adapter	16Gb	02.02.05	9.14.00	7.25	3.68
HPE SN1100Q 16GB Single Port PCIe Fibre Channel Host Bus Adapter	16Gb	02.02.05	9.14.00	7.25	3.68
HPE SN1600Q 32Gb Single Port Fibre Channel Host Bus Adapter	32Gb	02.02.05	9.14.00	7.25	3.68
HPE SN1600Q 32Gb Dual Port Fibre Channel Host Bus Adapter	32Gb	02.02.05	9.14.00	7.25	3.68
HPE SN1610Q 32Gb Dual Port Fibre Channel Host Bus Adapter	32Gb	02.09.07	09.14.01	7.36	0.0
HPE SN1610Q 32Gb Single Port Fibre Channel Host Bus Adapter	32Gb	02.09.07	09.14.01	7.36	0.0
HPE SN1700Q 64Gb Dual Port Fibre Channel Host Bus Adapter	64Gb	02.09.07	09.14.01	7.36	0.0
HPE SN1700Q 64Gb Single Port Fibre Channel Host Bus Adapter	64Gb	02.09.07	09.14.01	7.36	0.0

Prerequisites

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

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

Enhancements

This Firmware package contains following firmware versions:

Adapter	Speed	MBI	Firmware	UEFI	Boot Bios
HPE SN1100Q 16GB Dual Port PCIe Fibre Channel Host Bus Adapter	16Gb	02.02.05	9.14.00	7.25	3.68
HPE SN1100Q 16GB Single Port PCIe Fibre Channel Host Bus Adapter	16Gb	02.02.05	9.14.00	7.25	3.68
HPE SN1600Q 32Gb Single Port Fibre Channel Host Bus Adapter	32Gb	02.02.05	9.14.00	7.25	3.68
HPE SN1600Q 32Gb Dual Port Fibre Channel Host Bus Adapter	32Gb	02.02.05	9.14.00	7.25	3.68
HPE SN1610Q 32Gb Dual Port Fibre Channel Host Bus Adapter	32Gb	02.09.07	09.14.01	7.36	0.0
HPE SN1610Q 32Gb Single Port Fibre Channel Host Bus Adapter	32Gb	02.09.07	09.14.01	7.36	0.0
HPE SN1700Q 64Gb Dual Port Fibre Channel Host Bus Adapter	64Gb	02.09.07	09.14.01	7.36	0.0
HPE SN1700Q 64Gb Single Port Fibre Channel Host Bus Adapter	64Gb	02.09.07	09.14.01	7.36	0.0

Supported Devices and Features

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

16Gb Fibre Channel Host Bus Adapter:

- HPE SN1100Q 16GB Dual Port PCIe Fibre Channel Host Bus Adapter
- HPE SN1100Q 16GB Single Port PCIe Fibre Channel Host Bus Adapter

32Gb Fibre Channel Host Bus Adapter:

- HPE SN1600Q 32Gb Single Port Fibre Channel Host Bus Adapter
- HPE SN1600Q 32Gb Dual Port 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

64Gb Fibre Channel Host Bus Adapter:

- HPE SN1700Q 64Gb Dual Port Fibre Channel Host Bus Adapter
- HPE SN1700Q 64Gb Single Port Fibre Channel Host Bus Adapter

---

Software - Management Top

HPE Fiber Channel and Storage Enablement Bundle Smart Component for ESXi 8.0
Version: 2022.09.01 **(Recommended)**
Filename: cp051152.compsig; cp051152.zip

Enhancements

Supports VMware ESXi 8.0

HPE iLO Driver Bundle Smart Component for ESXi 7.0
Version: 2024.03.00 **(Recommended)**
Filename: cp059540.compsig; cp059540.zip

Fixes

This product addressed a memory leak in vmkernel.

Smart Storage Administrator (SSA) CLI Smart Component for ESXi 8.0 for Gen10/Gen10 Plus/Gen11 Controllers
Version: 2024.04.01 **(Recommended)**
Filename: cp058584.compsig; cp058584.zip

Fixes

- Fixed issue of ADU report generation when using SSADUESXI within the VMWare ESXi system.
- Fixed the display issue with physical drives in the enclosure under the multipath configuration.
- Fixed issue where the tool allowed the Heal array operation on RMSED secured arrays when KMS is not active.
- Fixed issue where the tools would allow users to attempt Change Drive Type operations with 512/512e drives for 4Kn logical volumes.
- Fixed issue where users specified an incorrect encryption mode for a logical volume that did not match the existing mode on the array.
- Fixed issue where the operation to revert the SEDs to Original Factory State (OFS) was not being blocked when KMS is not available in remote SED mode.
- Fixed the volume creation issue when users specify the 'volatileencryptionkey' option while the Controller setting does not support it.
- Fixed issue of error message occurring when using the 'create type=arrayR0' command with 'drives=' and 'drivetype=' options.
- Fixed installation issue encountered when attempting to downgrade SSACLI from versions 6.30.X.X to 6.15.X.X or 6.20.X.X.

Enhancements

- Added command to support the erasure of logs and events stored in the controller.
- Added command to support spare spin down policy setting if the feature is supported.

Software - Storage Controller Top

HPE MegaRAID Storage Administrator StorCLI for VMware8.0 (For Gen10P and Gen11 Controllers)
Version: 2023.12.01 **(Recommended)**
Filename: cp057483.compsig; cp057483.zip

Enhancements

- Support autoconfig command.

  storcli /cx set autoconfig = < none | JBOD >

- Added a new option [ReuseTargetId] to add vd command. If "ReuseTargetId" is mentioned in the add vd command, the FW will allow reusing of TargetIDs without 120 seconds delay.
- Added support for UBM7 backplanes.

Software - Storage Fibre Channel **Top**

HPE QLogic Fibre Channel driver component for VMware vSphere 8.0
Version: 2023.10.01 **(Recommended)**
Filename: cp058494.compsig; cp058494.zip

Important Note!

Release Notes:
HPE QLogic Adapters Release Notes

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

Prerequisites

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

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

Enhancements

Driver version 5.4.82.0

Supported Devices and Features

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

16Gb Fibre Channel Host Bus Adapter:

- HPE SN1100Q 16GB Dual Port PCIe Fibre Channel Host Bus Adapter
- HPE SN1100Q 16GB Single Port PCIe Fibre Channel Host Bus Adapter

32Gb Fibre Channel Host Bus Adapter:

- HPE SN1600Q 32Gb Single Port Fibre Channel Host Bus Adapter
- HPE SN1600Q 32Gb Dual Port 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

64Gb Fibre Channel Host Bus Adapter:

- HPE SN1700Q 64Gb Dual Port Fibre Channel Host Bus Adapter
- HPE SN1700Q 64Gb Single Port Fibre Channel Host Bus Adapter

---

Software - System Management **Top**

HPE Fiber Channel and Storage Enablement Component for ESXi 8.0
Version: 3.9.0 **(Recommended)**
Filename: fc-enablement-component_800.3.9.0.30-1_20300413.zip

Enhancements

Supports VMware ESXi 8.0

Get connected

hpe.com/info/getconnected

Current HPE driver, support, and security alerts delivered directly to your desktop

Updated May 07 2024

Hewlett Packard Enterprise