Release Notes for Cisco UCS Rack Server Software, Release 4.0(2)

First Published: 2019-01-02

Last Modified: 2021-06-28

Cisco UCS C-Series and S-Series Servers

Cisco UCS C-Series and S-Series Servers deliver unified computing in an industry-standard form factor to reduce total cost of ownership and increase agility. Each product addresses varying workload challenges through a balance of processing, memory, I/O, and internal storage resources.

About the Release Notes

This document describes the new features, system requirements, open caveats and known behaviors for C-Series and S-Series software release 4.0(2) including Cisco Integrated Management Controller software and any related BIOS, firmware, or drivers. Use this document in conjunction with the documents listed in the Related Documentation section.

Note We sometimes update the documentation after original publication. Therefore, you should also refer to the documentation on Cisco.com for any updates.

Revision History

Revision	Date	Description
P0	June 28, 2021	Following changes were made: • Updated the Resolved Caveats section. • Updated the HUU version to 4.0(2r). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.0

Revision	Date	Description
N0	March 18, 2021	Following changes were made: • Updated Supported Features section. • Updated the Resolved Caveats section. • Updated the HUU version to 4.0(2q). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.0
M1	February 01, 2021	Added Downgrade Limitation for Cisco UCS C125 M5 Servers.
M0	January 19, 2021	Following changes were made: • Updated Supported Features section. • Updated the HUU version to 4.0(2p). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.0
L0	November 03, 2020	Following changes were made: • Updated the Resolved Caveats section. • Updated the HUU version to 4.0(2o). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.0

Revision	Date	Description
K0	August 17, 2020	Following changes were made: • Updated the Security Fixes section. • Updated the Resolved Caveats section. • Updated the HUU version to 4.0(2n). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.0
I1	July 13, 2020	Following changes were made: • Updated the Known Behaviors section.
J0	May 05, 2020	Following changes were made: • Updated the Supported Features section.
I0	December 20, 2019	Following changes were made: • Updated the Supported Features section. Updated the Resolved Caveats section. • Updated the HUU version to 4.0(2m). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.0

Revision	Date	Description
H0	December 09, 2019	Following changes were made: • Updated the Security Fixes section. • Updated the HUU version to 4.0(2l). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.0
G0	November 04, 2019	Following changes were made: • Updated the Resolved Caveats section. • Updated the Known Behaviors section. • Updated the HUU version to 4.0(2k). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.0
F0	September 26, 2019	Following changes were made: • Updated the Resolved Caveats section. • Updated the HUU version to 4.0(2i). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.0

Revision	Date	Description
E0	August 01, 2019	Following changes were made: • Updated the Resolved Caveats section. • Updated the Security Fixes section. • Updated the HUU version to 4.0(2h). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.0
D0	May 15, 2019	Following changes were made: • Updated the Resolved Caveats section. • Updated the New Hardware section. • Updated the HUU version to 4.0(2g). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.0
C0	March 13, 2019	Following changes were made: • Updated the Resolved Caveats section. • Updated the HUU version to 4.0(2f). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.0

Revision	Date	Description
B0	January 17, 2019	Following changes were made: • Updated the Resolved Caveats section. • Updated the HUU version to 4.0(2d). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.0
A0	January 02, 2019	Created release notes for 4.0(2c).

Supported Platforms and Release Compatibility Matrix

Supported Platforms in this Release

The following servers are supported in this release:

- UCS C480 M5 ML
- UCS C125 M5
- UCS C220 M5
- UCS C240 M5
- UCS C480 M5
- UCS S3260 M5
- UCS S3260 M4
- UCS C220 M4
- UCS C240 M4
- UCS C460 M4

For information about these servers, see Overview of Servers

Cisco IMC and Cisco UCS Manager Release Compatibility Matrix

Cisco UCS C-Series and S-Series Rack-Mount Servers are managed by built-in standalone software —Cisco IMC. However, when a Rack-Mount Server is integrated with Cisco UCS Manager, the Cisco IMC does not manage the server anymore.

The following table lists the supported platforms, Cisco IMC releases, and Cisco UCS Manager releases for Rack-Mount Servers:

Table 1: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.0(2) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.0(2r)	No support	Cisco UCS C220 M4, C240 M4, and C460 M4 servers.
4.0(2q)	4.0(4l)	Cisco UCS C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.0(2p)	No support.	Cisco UCS C125 M5 servers
4.0(2o)	4.0(4j)	Cisco UCS C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.0(2n)	No support.	Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.0(2m)	No support.	Cisco UCS S3260 M4 and M5 servers
4.0(2l)	No support.	Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.0(2k)	No support.	Cisco UCS S3260 M4 and M5 servers
4.0(2i)	No support.	Cisco UCS C460 M4, S3260 M4, and S3260 M5 servers
4.0(2h)	4.0(2e)	Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.0(2f)	4.0(2d)	Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.0(2d)	4.0(2b)	Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.0(2c)	4.0(2a)	Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers

Table 2: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.0(1) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.0(1e)	No support.	Cisco UCS M4, M5 servers and C125 M5
4.0(1d)	4.0(1d)	Cisco UCS M4, M5 servers and C125 M5
4.0(1c)	4.0(1c)	Cisco UCS M4, M5 servers and C125 M5
4.0(1b)	4.0(1b)	Cisco UCS M4, M5 servers and C125 M5
4.0(1a)	4.0(1a)	Cisco UCS M4, M5 servers and C125 M5

Table 3: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 3.1(3) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
3.1(3k)	3.2(3p)	Cisco UCS C480 M5, C220 M5, C240 M5, and S3260 M5 servers
3.1(3j)	No Support **Note** We support discovery and upgrade or downgrade functions with Cisco UCS Manager.	Cisco UCS C480 M5, C220 M5, C240 M5, and S3260 M5 servers
3.1(3i)	3.2(3i)	Cisco UCS C480 M5, C220 M5, C240 M5, and S3260 M5 servers
3.1(3h)	3.2(3h)	Cisco UCS C480 M5, C220 M5, C240 M5, and S3260 M5 servers
3.1(3g)	3.2(3g)	Cisco UCS C480 M5, C220 M5, C240 M5, and S3260 M5 servers
3.1(3d)	3.2(3e)	Cisco UCS C480 M5, C220 M5, C240 M5, and S3260 M5 servers
3.1(3c)	3.2(3d)	Cisco UCS C480 M5, C220 M5, C240 M5, and S3260 M5 servers
3.1(3b)	3.2(3b)	Cisco UCS C480 M5, C220 M5, and C240 M5 servers
3.1(3a)	3.2(3a)	Cisco UCS C480 M5, C220 M5, C240 M5, and S3260 M5 servers

Table 4: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 3.1(2) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
3.1(2d)	3.2(2d)	Cisco UCS C480 M5, C220 M5, and C240 M5
3.1(2c)	3.2(2c)	Cisco UCS C480 M5, C220 M5, and C240 M5
3.1(2b)	3.2(2b)	Cisco UCS C480 M5, C220 M5, and C240 M5

Table 5: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 3.1(1) Release

C-Series Standalone Release	Cisco UCS Manager Release	C-Series Servers
3.1(1d)	3.2(1d)	Cisco UCS C220 M5/C2540 M5

Table 6: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 3.0(4) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack-Mount Servers
3.0(4s)	No support	Cisco UCS C220 M3, C240 M3, C3160 M3, S3260 M4
3.0(4r)	No support	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3
3.0(4q)	No support	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3
3.0(4p)	3.2(3o)	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3
3.0(4o)	No support	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3
3.0(4n)	No support.	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3

Cisco IMC Release	Cisco UCS Manager Release	Rack-Mount Servers
3.0(4m)	No support.	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3
3.0(4l)	No support.	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3
3.0(4k)	No support.	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3
3.0(4j)	3.1(3k)	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3
3.0(4i)	3.1(3j)	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3
3.0(4e)	No support	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3
3.0(4d)	3.1(3h)	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3
3.0(4a)	3.1(3f)	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3

Table 7: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 3.0(3) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack-Mount Servers
3.0(3f)	-	Cisco UCS C240 M4, and C220 M4
3.0(3e)	3.0(3e)	Cisco UCS C22 M3, C24 M3, C220 M3, C240 M3, C220 M4, C240 M4, C460 M4, C3160 M3, S3260 M4 and S3260 M3 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack-Mount Servers
3.0(3c)	3.0(3c)	Cisco UCS C240 M4, and C220 M4
3.0(3b)	3.0(3b)	Cisco UCS S3260 M3, C3160 M3, C460 M4, C240 M4, and C220 M4
3.0(3a)	3.1(3a)	Cisco UCS C22 M3, C24 M3, C220 M3, C240 M3, C220 M4, C240 M4, C460 M4, C3160 M3, S3260 M4 and S3260 M3 servers

Table 8: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 3.0(2) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack-Mount Servers
3.0(2b)	No Support **Note** We support discovery and upgrade or downgrade functions with Cisco UCS Manager.	C220 M4/C240 M4 only

Table 9: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 3.0(1) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack-Mount Servers
3.0(1d)	No Support **Note** We support discovery and upgrade or downgrade functions with Cisco UCS Manager.	All M3/M4 except C420 M3
3.0(1c)	No Support	All M3/M4 except C420 M3

Cisco IMC Release	UCS Manager Release	Rack Mount Servers
2.0(13e)	3.1(2b)	All M3/M4 except C420 M3
2.0(10b)	3.1(1g)	C220 M4/C240 M4 only
2.0(9c)	3.1(1e)	All other M3/M4
2.0(9f)	2.2(7b)	For all other M3/M4
2.0(10b)	2.2(7b)	C220 M4/C240 M4 only
1.5(9d)	2.2(7b)	C420-M3, C260-M2, C460-M2 only

Cisco IMC Release	UCS Manager Release	Rack Mount Servers
1.5(9d)	2.2(8f)	C420-M3, C260-M2, C460-M2 only
2.0(9c)	2.2(8f)	For all other M3/M4
2.0(10b)	2.2(8f)	C220 M4/C240 M4 only
2.0(12b)	2.2(8f)	C460 M4 only
1.5(8a)	2.2(6g)	C420 M3, C260 M2, C460 M2 only
2.0(8d)	2.2(6c)	For all other M3/M4
1.5(7f)	2.2(5b)	C420 M3, C260 M2, C460 M2 only
2.0(6d)	2.2(5a)	For all other M3/M4
1.5(7a)2	2.2(4b)	C420 M3, C260 M2, C460 M2 only
2.0(4c)	2.2(4b)	For all other M3/M4
1.5(7c)1	2.2(3b)	C420 M3, C260 M2, C460 M2 only
2.0(3d)1	2.2(3a)	For all other M3/M4

Operating System and Browser Requirements

For detailed information about supported Operating System, see the interactive UCS Hardware and Software Compatibility matrix.

Cisco recommends the following browsers for Cisco UCS Rack Server Software, Release 4.0(2):

- Sun JRE 1.8.0_92 or later
- HTML based interfaces are supported on:
  - Microsoft Internet Explorer 10.0 or 11
  - Mozilla Firefox 47.0 or higher
  - Google Chrome 38 or higher
  - Safari 7 or higher

Note If the management client is launched using an unsupported browser, check the help information from the **For best results use supported browsers** option available in the login window for the supported browser versions.

- Transport Layer Security (TLS) version 1.2.

Hardware and Software Interoperability

For detailed information about storage switch, operating system and adapter, see the *Hardware and Software Interoperability Matrix* for your release located at:

http://www.cisco.com/en/US/products/ps10477/prod_technical_reference_list.html

Note Connectivity is tested between the server and the first connected device. Further connections, such as to storage arrays after a switch are not listed in the Cisco UCS Hardware Compatibility List though they may be highlighted in the vendor support matrix for those devices.

For details about transceivers and cables that are supported on VIC cards, see the Transceiver Modules Compatibility Matrix

You can also see the VIC data sheets for more compatibility information: Cisco UCS Virtual Interface Card Data Sheets

Upgrade Paths to Release 4.0

The section provides information on the upgrade paths to release 4.0. Refer to the table for upgrade paths for various Cisco UCS C-series IMC versions.

Table 10: Upgrade Paths to Release 4.0

Upgrade From Release	Upgrade To Release	Recommended Upgrade Path
All M5 Servers from 3.1	4.0	Follow below upgrade path: • You can use Interactive HUU or Non-Interactive HUU (NIHUU) script to update the server. • While updating the firmware using the NIHUU tool, use the Python scripts that are released with version 4.0. • Use OpenSSL 1.0.1e-fips on the client side (where the NIHUU python scripts are running). • Download HUU iso from here. • Download NIHUU script from here.

Upgrade From Release	Upgrade To Release	Recommended Upgrade Path
For all M4 servers for releases greater than 3.0(3a)	4.0	Follow these steps to upgrade from releases greater than 3.0(3a) to 4.0: • You can use Interactive HUU or NIHUU script to update the server. • While updating the firmware using the NIHUU tool, use the Python scripts that are released with version 4.0. • Use OpenSSL 1.0.1e-fips on the client side (where the NIHUU python scripts are running). • If you wish to secure Cimc Boot, set flag **use_cimc_secure** as **yes** in **multiserver_config** file present with python script. • Download HUU iso from here. • Download NIHUU script from here.

Upgrade From Release	Upgrade To Release	Recommended Upgrade Path
For all M4 servers for release lesser than 3.0(3a) except C460 M4 For C460 M4 servers for release 2.0(4c) to 3.0(3a)	4.0	Follow these steps to upgrade from releases less than 3.0(3a) to 4.0: **Upgrade from version less than 3.0(3a) to 3.0(3a)** • You can use Interactive HUU or NIHUU script to update the server. • While updating the firmware using the Non-Interactive HUU (NIHUU) tool, use the Python scripts that are released with version 3.0(3a). • Use OpenSSL 1.0.1e-fips on the client side (where the NIHUU python scripts are running). • Download HUU iso from here. • Download NIHUU script from here. **Upgrade from 3.0(3a) to 4.0** • You can use Interactive HUU or NIHUU script to update the server. • While updating the firmware using the NIHUU tool, use the Python scripts that are released with version 4.0. • Use OpenSSL 1.0.1e-fips on the client side (where the NIHUU python scripts are running). • If you wish to secure Cimc Boot, set flag **use_cimc_secure** as **yes** in **multiserver_config** file present with python script. • Download HUU iso from here. • Download NIHUU script from here.

Upgrade From Release	Upgrade To Release	Recommended Upgrade Path
For C460 M4 servers for release lesser than 2.0(4c)	4.0	

Upgrade From Release	Upgrade To Release	Recommended Upgrade Path
		Follow these steps to upgrade from releases less than 2.0(4c) to 4.0: Upgrade from version less than 2.0(4c) to 2.0(4c) • You can use Interactive HUU or NIHUU script to update the server. • While updating the firmware using the NIHUU tool, use the Python scripts that are released with version 2.0(4c). • Use OpenSSL 1.0.0-fips on the client side (where the NIHUU python scripts are running). • If you wish to secure Cimc Boot, set flag **use_cimc_secure** as **yes** in **multiserver_config** file present with python script. • Download HUU iso from here. • Download NIHUU script from here. **Upgrade from 2.0(4c) to 3.0(3a)** • You can use Interactive HUU or NIHUU script to update the server. • While updating the firmware using the NIHUU tool, use the Python scripts that are released with version 3.0(3a). • Use OpenSSL 1.0.1e-fips on the client side (where the NIHUU python scripts are running). • If you wish to secure Cimc Boot, set flag **use_cimc_secure** as **yes** in **multiserver_config** file present with python script. • Download HUU iso from here. • Download NIHUU script from here. **Upgrade from 3.0(3a) to 4.0** • You can use Interactive HUU or NIHUU script to update the server. • While updating the firmware using the NIHUU tool, use the Python scripts that are released with version 4.0.

Upgrade From Release	Upgrade To Release	Recommended Upgrade Path
		- Use OpenSSL 1.0.1e-fips on the client side (where the NIHUU python scripts are running). - If you wish to secure Cimc Boot, set flag **use_cimc_secure** as **yes** in **multiserver_config** file present with python script. - Download HUU iso from here. - Download NIHUU script from here.

Firmware Upgrade Details

Firmware Files

The C-Series software release 4.0(2) includes the following software files:

CCO Software Type	File name(s)	Comment
Unified Computing System (UCS) Server Firmware	ucs-c480m5-huu-4.0.2.iso ucs-c125-huu-4.0.2.iso ucs-c240m5-huu-4.0.2.iso ucs-c220m5-huu-4.0.2.iso ucs-s3260-huu-4.0.2.iso ucs-c240m4-huu-4.0.2.iso ucs-c220m4-huu-4.0.2.iso ucs-c460m4-huu-4.0.2.iso For release specific ISO versions, see Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.0	Host Upgrade Utility
Unified Computing System (UCS) Drivers	ucs-cxxx-drivers.4.0.2.iso	Drivers
Unified Computing System (UCS) Utilities	ucs-cxxx-utils-efi.4.0.2.iso ucs-cxxx-utils-linux.4.0.2.iso ucs-cxxx-utils-vmware.4.0.2.iso ucs-cxxx-utils-windows.4.0.2.iso	Utilities

Note Always upgrade the BIOS, the Cisco IMC and CMC from the HUU ISO. Do not upgrade individual components (only BIOS or only Cisco IMC), since this could lead to unexpected behavior. If you choose to upgrade BIOS, and the Cisco IMC individually and not from the HUU ISO, make sure to upgrade both Cisco IMC, and BIOS to the same container release. If the BIOS and the Cisco IMC versions are from different container releases, it could result in unexpected behavior. Cisco recommends that you use the Update All option from the Host Upgrade Utility to update the firmware versions of Cisco IMC, BIOS, and all other server components (VIC, RAID Controllers, PCI devices, and LOM) together.

Host Upgrade Utility

The Cisco Host Upgrade Utility (HUU) is a tool that upgrades the Cisco UCS C-Series firmware.

The image file for the firmware is embedded in the ISO. The utility displays a menu that allows you to choose which firmware components to upgrade. For more information on this utility see:

http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html

For details of firmware files in Cisco Host Upgrade Utility for individual releases, see Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.0

Updating the Firmware

Use the Host Upgrade Utility to upgrade the C-Series firmware. Host Upgrade Utility can upgrade the following software components:

- BIOS
- Cisco IMC
- CMC
- Cisco VIC Adapters
- DCPMM Memory
- LSI Adapters
- LAN on Motherboard
- PCIe adapter firmware
- HDD firmware
- SAS Expander firmware

For detailed information about the components available in a server for each release, see: Cisco UCS C-Series Integrated Management Controller Firmware Files

All firmware should be upgraded together to ensure proper operation of your server.

Note We recommend that you use the **Update All** option from the Host Upgrade Utility to update the firmware versions of Cisco IMC, BIOS and all other server components (VIC, RAID Controllers, PCI devices, and LOM) together. Click **Exit** once you deploy the firmware.

For more information on how to upgrade the firmware using the utility, see:

Cisco Host Upgrade Utility User Guide

Downgrade Limitation

Downgrade Limitation for Cisco UCS C125 M5 Servers

Release 4.0(2p) introduces AMD Platform Secure Boot (PSB) in Cisco UCS C125 M5 servers that implements hardware-rooted boot integrity. Once you upgrade, you cannot downgrade Cisco UCS C125 M5 Rack Server Node based on AMD EPYC 7001 (Naples) to any release earlier than 4.0(2p).

Supported Features

Supported Features

Release 4.0(2q)

The following new software feature is supported in Release 4.0(2q):

- **Panic and High Watermark** BIOS token is added for Cisco UCS C220 M4, C240 M4, C460 M4, and S3260 M4 servers. For more information, see Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide, Release 4.0 or Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Release 4.0 at Configuration Guides.

Release 4.0(2p)

The following new software feature is supported in Release 4.0(2p):

- Release 4.0(2p) introduces AMD Platform Secure Boot (PSB) in Cisco UCS C125 M5 servers that implements hardware-rooted boot integrity. PSB ensures the integrity and authenticity of ROM image by using the root of trust integrated in the hardware.

Release 4.0(2m)

Firmware for the following HDD models are updated in release 4.0(2m):

- HUH721008AL4200—Firmware updated to version A3Z4
- HUH721010AL42C0—Firmware updated to version A3Z4
- HUH721010AL5200—Firmware updated to version A3Z4
- HUH721010AL52C0—Firmware updated to version A3Z4
- HUH721010AL4200—Firmware updated to version A3Z4

Release 4.0(2d)

The following new software feature is supported in Release 4.0(2d):

- Added support to update the device connector firmware version using the CLI and XML API commands.

Release 4.0(2c)

The following new software features are supported in Release 4.0(2c):

- Added the **Certificate Manager** feature that allows you to view a list of trusted certificates and import a valid trusted certificate.
- **Single IP Properties**—Added an option to configure the single IP properties that enables assigning IPv4 addresses to Cisco IMC management.

  Note This feature is available only on the S3260 servers.

- **PCI Switch Updates**—Added options to view the information about the PCI Switches present and also view the details of a particular PCI Switch.

  Note Option to view details of a particular switch is available only on the C480 M5 ML servers.

- **vNIC Configuration Updates**—Added an option to enable and configure the **Multi Queues** on vNICs.
- **VMMQ Windows Support**—Added VMMQ support for Windows 2016 and above for VIC 14xx series adapters.
- **vHBA Configuration Updates**—Added an option to configure **vHBA Type**. The configuration options include:
  - **fc-initiator**
  - **fc-target**
  - **fc-nvme-initiator**
  - **fc-nvme-target**
- **NVMe over FC Support**—Added NVMe over FC support for the VIC 14xx series adapters.
- **Changing Password of a Non-Admin User**—Added a feature that allows users with read-only user privileges to change the password.

  Note This option is not available for admin users.

- **BIOS Token Updates**—Added the **BIOS Techlog Level** and **OptionROM Launch Optimization** BIOS tokens.
- **Virtual KVM Console Updates:**—Added options to view the statistics of the KVM sessions and option to reset the USB connections.

New Hardware in Release 4.0(2)

Release 4.0(2g)

The following new hardware was added in release 4.0(2g):

Support for Intel® XXV710 25G 2-port SFP PCIe adapter (UCSC-PCIE-ID25GF) on C125 M5 servers.

Release 4.0(2c)

The following new hardware was added in release 4.0(2c):

Cisco UCS C480 M5 ML Server

The Cisco UCS C480 M5 ML Rack Server is a purpose-built server for Deep Learning. It is storage- and I/O-optimized for training models. The Cisco UCS C480 M5 ML Server delivers outstanding levels of storage expandability and performance options for standalone or Cisco UCS-managed environments in a 4RU form factor. It offers these capabilities:

- 8 NVIDIA SXM2 V100 32G modules with NVLink interconnect
- Latest Intel® Xeon® Scalable processors with up to 28 cores per socket and support for two processor configurations
- 2666-MHz DDR4 memory and 24 DIMM slots for up to 3 terabytes (TB) of total memory
- 4 PCI Express (PCIe) 3.0 slots for up to 4 10/25 or 40/100G Cisco VICs (VIC 1455 and VIC 1495)
- Flexible storage options with support for up to 24 Small-Form-Factor (SFF) 2.5-inch, SAS/SATA Solid-State Disks (SSDs) and Hard-Disk Drives (HDDs)
- Up to 6 PCIe NVMe disk drives
- Cisco 12-Gbps SAS Modular RAID Controller in a dedicated slot
- M.2 boot options
- Dual embedded 10 Gigabit Ethernet LAN-On-Motherboard (LOM) ports

UCS VIC 1400 Series Adapters

Support for the following new UCS VIC 1400 Series adapters on UCS M5 servers and UCS C125 M5 servers:

- VIC 1495 40/100G PCIe for C-Series (UCSC-PCIE-C100-04)
- VIC 1497 40/100G mLOM for C-Series (UCSC-MLOM-C100-04)

Note You cannot install VIC adapters from different series on the same server. For example, you cannot install UCS VIC 1300 Series adapters and UCS VIC 1400 Series adapters on the same server.

For more details regarding server and adapter combinations, refer the Server Spec Sheets:

- C-Series Server Spec Sheets
- S-Series Server Spec Sheets

Peripherals

- Support for TPM2 (UCSX-TPM2-002-C) for all UCS servers.
- Support for Intel® Optane™ NVMe Extreme Performance Drives (UCSC-NVMEXP-I750)
- Support for the QLogic FastLinQ QL41132HORJ Dual-port 10G Network Adapter card (UCSC-PCIE-QD10GC) on UCS C125 M5 servers.
- Support for the QLogic FastLinQ QL41232HOCU Dual-port 25G Network Adapter card (UCSC-PCIE-QD25GF) on UCS C125 M5 servers.
- Support for the QLogic FastLinQ QL45611H 100GbE Network Adapter card (UCSC-PCIE-QS100GF) on UCS C480 M5 ML.
- Support for NVIDIA V100 PCIe PG500-200 250W 32GB GPU card (UCSC-GPU-V100-32) on UCS C240 M5 servers.
- Support for AMD Radeon Pro V340, 2X16GB, 300W GPU cards (UCSC-GPU-V340) on UCS C240 M5 servers.

Software Utilities

The following standard utilities are available:

- Host Update Utility (HUU)
- BIOS and Cisco IMC Firmware Update utilities
- Server Configuration Utility (SCU)
- Server Diagnostic Utility (SDU)

The utilities features are as follows:

- Availability of HUU, SCU on the USB as bootable images. The USB also contains driver ISO, and can be accessed from the host operating system.

SNMP

The supported MIB definition for this release and later releases can be found at the following link:

ftp://ftp.cisco.com/pub/mibs/supportlists/ucs/ucs-C-supportlist.html

Note The above link is incompatible with IE 9.0.

Security Fixes in Release 4.0(2)

Security Fixes in Release 4.0(2n)

The following Security Fix was added in Release 4.0(2n):

Release	Defect ID	CVE	Symptom
4.0(2n)	CSCvs31877	• CVE-2019-0139 • CVE-2019-0140 • CVE-2019-0142 • CVE-2019-0143 • CVE-2019-0144 • CVE-2019-0145 • CVE-2019-0146 • CVE-2019-0147 • CVE-2019-0148 • CVE-2019-0149 • CVE-2019-0150	

Release	Defect ID	CVE	Symptom
			Cisco UCS C-Series and S-Series M5 servers, which include an Intel® Ethernet 700 Series Controller are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs: • CVE-2019-0139 affects controllers running firmware versions earlier than 7.0. Due to insufficient access control in the firmware, this vulnerability may allow a privileged user to potentially enable an escalation of privilege, denial of service, or information disclosure through local access. • CVE-2019-0140 affects controllers running firmware versions earlier than 7.0. Due to buffer overflow in the firmware, this vulnerability may allow an unauthenticated user to potentially enable an escalation of privilege through an adjacent access. • CVE-2019-0142 affects controllers running firmware versions earlier than 1.33.0.0. Due to insufficient access control in the `ilp60x64.sys` driver, this vulnerability may allow a privileged user to potentially enable escalation of privilege through local access. • CVE-2019-0143 affects controllers running firmware versions earlier than 7.0. Due to unhandled exceptions in kernel-mode drivers, this vulnerability may allow an authenticated user to potentially enable a denial of service through local access. • CVE-2019-0144 affects controllers running firmware versions earlier than 7.0. Due to unhandled exceptions in firmware, this vulnerability may allow an authenticated user to potentially enable a denial of service through local access. • CVE-2019-0145 affects controllers running firmware versions earlier than 2.8.43. Due to buffer overflow in `i40e` drivers, this vulnerability may allow an authenticated user to potentially enable an escalation of privilege through local access. • CVE-2019-0146 affects controllers running firmware versions earlier than 2.8.43. Due to resource leak in `i40e` drivers, this vulnerability may allow an authenticated user to potentially

Release	Defect ID	CVE	Symptom
			enable a denial of service through local access. • CVE-2019-0147 affects controllers running firmware versions earlier than 7.0. Due to insufficient input validation in `i40e` drivers, this vulnerability may allow an authenticated user to potentially enable a denial of service through local access. • CVE-2019-0148 affects controllers running firmware versions earlier than 7.0. Due to resource leak in `i40e` drivers, this vulnerability may allow an authenticated user to potentially enable a denial of service through local access. • CVE-2019-0149 affects controllers running firmware versions earlier than 2.8.43. Due to insufficient input validation in `i40e` drivers, this vulnerability may allow an authenticated user to potentially enable a denial of service through local access. • CVE-2019-0150 affects controllers running firmware versions earlier than 7.0. Due to insufficient access control in firmware, this vulnerability may allow a privileged user to potentially enable a denial of service through local access.

Security Fixes in Release 4.0(2l)

The following Security Fix was added in Release 4.0(2l):

Release	Defect ID	CVE	Symptom
4.0(2l)	CSCvr54416	• CVE-2019-0151 • CVE-2019-11137	Cisco UCS C-Series and S-Series M4 servers that are based on Intel® processors are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs: • CVE-2019-0151 (CPU Local Privilege Escalation Advisory) affects certain Intel® 4th Generation Intel® Core™ Processors, 5th Generation Intel® Core™ Processors, 6th Generation Intel® Cores Processors, 7th Generation Intel® Core™ Processors, 8th Generation Intel® Core™ Processors, Intel® Xeon® Processors E3 v2/v3/v4/v5/v6 Family, Intel® Xeon® Processors E5 v3/v4 Family, Intel® Xeon® Processors E7 v3/v4 Family, Intel® Xeon® Scalable Processors 2nd Generation, Intel® Xeon® Scalable Processors, Intel® Xeon® Processors D-1500/D-2100), Intel® Xeon® Processors E-2100/E3100, and, Intel® Xeon® Processors W-2100/W-3100 when insufficient memory protection in Intel® TXT may allow a privileged user to potentially enable escalation of privilege through local access. This could result in bypassing Intel® TXT protections. • CVE-2019-11137 (BIOS 2019.2 IPU Advisory) affects 2nd Generation Intel® Xeon® Scalable Processors, Intel® Xeon® Scalable Processors, Intel® Xeon® Processor D Family, Intel® Xeon® Processor E5 v4 Family, Intel® Xeon® Processor E7 v4 Family, Intel® Atom® Processor C Series when insufficient input validation in the system firmware may allow a privileged user to potentially enable an escalation of privilege, denial of service, or information disclosure through local access. This release includes BIOS revisions for Cisco UCS M4 generation servers. These BIOS revisions include the updated microcode and Secure Initialization (SINIT) Authenticated Code Modules (ACM), which are required parts of the mitigation for these vulnerabilities.

Security Fixes in Release 4.0(2h)

The following Security Fix was added in Release 4.0(2h):

Release	Defect ID	CVE	Symptom
4.0(2h)	CSCvq66225	• CVE-2019-9836	On the Cisco UCS C-Series servers that are based on AMD EPYC™ processors, using the user-selectable AMD secure encryption feature on a virtual machine running the Linux operating system, an encryption key could be compromised by manipulating the encryption technology's behavior. This release includes the BIOS revision to mitigate this risk. For more information about this vulnerability, see https://www.amd.com/en/corporate/product-security

Security Fixes in Release 4.0(2g)

The following Security Fixes were added in Release 4.0(2g):

Release	Defect ID	CVE	Symptom
4.0(2g)	CSCvp34790 CSCvp34799	• CVE-2018-12126 • CVE-2018-12127 • CVE-2018-12130 • CVE-2019-11091	Cisco UCS C-Series and S-Series M4 servers are based on Intel® Xeon® Processor E7 v2, v3, and v4 Product Family processors that are vulnerable to variants of exploits that use Microarchitectural Data Sampling (MDS) to gain access to data being processed in the CPU by other applications. • CVE-2018-12126 (Microarchitectural Store Buffer Data Sampling) affects store buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Cisco IMC release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. • CVE-2018-12127 (Microarchitectural Load Port Data Sampling) affects load buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Cisco IMC release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. • CVE-2018-12130 (Microarchitectural Fill Buffer Data Sampling) affects line fill buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Cisco IMC release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. • CVE-2019-11091 (Microarchitectural Uncacheable Data Sampling) affects the uncacheable memory buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Cisco IMC release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. This release includes BIOS revisions for Cisco UCS M4 generation servers. These BIOS revisions include the updated microcode that is a required part of the mitigation for these vulnerabilities.

Release	Defect ID	CVE	Symptom
4.0(2g)	CSCvp34786	• CVE-2018-12126 • CVE-2018-12127 • CVE-2018-12130 • CVE-2019-11091	Cisco UCS C-Series and S-Series M4 servers are based on Intel® Xeon® Processor E5 v3 and v4 Product Family processors that are vulnerable to variants of exploits that use Microarchitectural Data Sampling (MDS) to gain access to data being processed in the CPU by other applications. • CVE-2018-12126 (Microarchitectural Store Buffer Data Sampling) affects store buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Cisco IMC release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. • CVE-2018-12127 (Microarchitectural Load Port Data Sampling) affects load buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Cisco IMC release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. • CVE-2018-12130 (Microarchitectural Fill Buffer Data Sampling) affects line fill buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Cisco IMC release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. • CVE-2019-11091 (Microarchitectural Uncacheable Data Sampling) affects the uncacheable memory buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Cisco IMC release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. This release includes BIOS revisions for Cisco UCS M4 generation servers. These BIOS revisions include the updated microcode that is a required part of the mitigation for these vulnerabilities.

Release	Defect ID	CVE	Symptom
4.0(2g)	CSCvp34806	• CVE-2018-12126 • CVE-2018-12127 • CVE-2018-12130 • CVE-2019-11091	Cisco UCS M5 servers are based on Intel® Xeon® Scalable processors that are vulnerable to variants of exploits that use Microarchitectural Data Sampling (MDS) to gain access to data being processed in the CPU by other applications. • CVE-2018-12126 (Microarchitectural Store Buffer Data Sampling) affects store buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Cisco IMC release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. • CVE-2018-12127 (Microarchitectural Load Port Data Sampling) affects load buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Cisco IMC release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. • CVE-2018-12130 (Microarchitectural Fill Buffer Data Sampling) affects line fill buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Cisco IMC release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. • CVE-2019-11091 (Microarchitectural Uncacheable Data Sampling) affects the uncacheable memory buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Cisco IMC release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. This release includes BIOS revisions for Cisco UCS M5 generation servers. These BIOS revisions include the updated microcode that is a required part of the mitigation for these vulnerabilities.

Security Fixes for Release 4.0(2c)

The following security fix was addressed in Release 4.0(2c):

Release	Defect ID	CVE	Description
4.0(2c)	CSCvm35067	CVE-2016-1549 CVE-2018-7184 CVE-2018-7170 CVE-2018-7185 CVE-2018-7182 CVE-2018-7183	Cisco Integrated Management Controller includes a version of ntpd that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs: CVE-2016-1549, CVE-2018-7184, CVE-2018-7170, CVE-2018-7185, CVE-2018-7182, CVE-2018-7183. This vulnerability was fixed in release 4.0(2c).

Resolved Caveats

The following section lists resolved caveats.

Resolved Caveats in Release 4.0(2)

Release 4.0(2r)

The following defect was resolved in release 4.0(2r):

Table 11: External LSI SAS Controller

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvs01145	In Cisco UCS C-Series M4 servers, HBA resets are observed during VM migration. After this, VM goes into read only mode. This issue is now resolved.	4.0(1e)	4.0(2r)

Release 4.0(2q)

The following defect was resolved in release 4.0(2q):

Table 12: BMC

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvw95072	NMPowerManager.c triggers an unexpected power off event during OS run time in Cisco UCS M5 servers. As a result, Cisco IMC shuts down the server and triggers power characterization. This issue is now resolved.	4.1(2b)	4.0(2q)

Release 4.0(2o)

The following defect was resolved in release 4.0(2o):

Table 13: BMC

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvv64567	UCS Manager fails to discover Cisco UCS S3260 M4 servers due to UCS Manager and BMC version mismatch. This issue is now resolved.	4.0(2o)	4.0(2o)

Release 4.0(2n)

The following defect was resolved in release 4.0(2n):

Table 14: BIOS

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvu93105	For Cisco UCS C125 M5 servers, modifying **Memory Interleaving** BIOS token from Cisco IMC or BIOS setup window does not trigger the feature functionality even though the BIOS token value is updated correctly. This issue is now resolved.	4.0(2m)	4.0(2n)

Table 15: BMC

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvr70687	New Cisco UCS C240 M5 server discovery fails or does not respond with the following error message: `CimcVMedia Error: Error retrieving vmedia attributes list-MC Error(-6)` The same issue may occur for any Cisco UCS C240 M5 server after an FI reboot or upgrade. This issue is now resolved.	4.0(4d)	4.0(2n)

Table 16: Host Firmware Upgrade

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvs48461	While upgrading Cisco IMC to 4.0(2m) or 4.0(4i) in Cisco UCS S3260 M5 and M4 servers, HUU and NIHUU report HDD firmware updates as failed, even after the actual update is successful. This issue is now resolved.	4.0(2m)	4.0(2n)

Table 17: VIC

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvm59040	Cisco UCS C220 servers with an up-time of over 180 days and equipped with Cisco UCS VIC 1225 may report loss of connectivity from the host. This issue is now resolved with the latest firmware version.	2.0(13f)	4.0(2n)

Release 4.0(2m)

The following defect was resolved in release 4.0(2m):

Table 18: Firmware Upgrade

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvr91935	On Cisco UCS S3260 M4 and M5 servers, the firmware activation of Cisco UCS VIC 1455 and 1495 cards failed after NI-HUU/HUU update. This issue is now resolved.	4.0(2k)	4.0(2m)

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvo18736	Intel X710 NIC firmware upgrade bundled with HUU version 4.0(2d) or later fails, causing disruption in network connectivity. This issue is now resolved.	4.0(2d) and later	4.0(2m)
CSCvr88803	NI-HUU script fails with `vmedia mapping has gone bad` error. The script may fail on a verify boot when the option: "`update_verify = yes`" is set in the configuration file. This issue is now resolved.	4.0(2k)	4.0(2m)
CSCvr71907	On S3260 M4 servers, NI-HUU firmware upgrade or downgrade may fail with the `timeout error`. When this happens firmware of only some components are updated and firmware of some components have to be updated again. This issue is now resolved.	4.0(2k)	4.0(2m)

Release 4.0(2l)

There are no resolved caveats in release 4.0(2l).

Release 4.0(2k)

The following defect was resolved in release 4.0(2k):

Table 19: Utilities

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvr61928	While updating the firmware on M4 and M5 servers using NI-HUU, CMC activation fails. This happens when there is no change in BIOS firmware version and there is change in BMC and CMC firmware versions.	4.0(1a)	4.0(2k)

Release 4.0(2i)

The following defects were resolved in release 4.0(2i):

Table 20: BIOS

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvo77732	After upgrading the UCS C460 M4 with Intel Xeon v2 CPUs to 4.0 firmware versions, the server crashes (PSOD), becomes unresponsive, or encounters a CATERR.	4.0(1c)	4.0(2i)

Table 21: Utilities

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvr07491	After upgrading the firmware of multiple S3260 servers using the Non-Interactive HUU, firmware activation fails for a few server components such as BMC, BIOS, CMC and SAS Expander.	4.0(1a)	4.0(2i)

Release 4.0(2h)

The following defect was resolved in release 4.0(2h):

Table 22: BIOS

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvo48006	On the M4 servers, uncorrectable ECC error detected during Patrol Scrub. When the CPU IMC (Integrated Memory Controller) Patrol Scrubber detects an uncorrectable ECC error, it logs a truncated DIMM address (4KB page boundary) to the Machine Check Banks.	4.0(2c)	4.0(2h)

Release 4.0(2g)

The following defects were resolved in release 4.0(2g):

Table 23: BMC

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvo15978	On servers with M393A4K40BB2-CTD DIMMs, IPMI may stop working. Errors related to temperature, CPU and/or DIMM mismatch in the management console, fan speed 100%, and chassis notifications are reported.	4.0(1a)	4.0(2g)
CSCvp41543	SSH clients fail to establish a connection to Cisco IMC. This happens when the SSH clients use `diffie-hellman-group14-sha1` as default KEX algorithm as support for this KEX algorithm has been removed from Cisco IMC. Update the SSH clients to the latest version that uses stricter KEX algorithms to establish SSH sessions.	3.0(4j)	4.0(2g)

Table 24: Firmware Upgrade

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvp34583	Firmware activation of VIC cards or UCSC-C3260-SIOC card fails for any release prior to 4.0(2c). This happens on all M4 and M5 servers that are in Cisco card mode.	Any release before 4.0(2c)	4.0(2g)

Release 4.0(2f)

The following defects were resolved in release 4.0(2f):

Table 25: BMC

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvn81570	Modifying the LUN ID for Flex Flash SD card VD fails with the following error: `error in configuring device`	4.0(1c)	4.0(2f)

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvn80088	Unable to initiate non-interactive HUU update when the remote share password provided in the NI HUU contains any of the following special characters ; | ? $! @ # % ^ * - _ +	4.0(1a)	4.0(2f)

Release 4.0(2d)

The following defects were resolved in release 4.0(2d):

Table 26: Utilities

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvn92435	Host Update Utility not booting on the following platform: BE7M-M5-K9. HUU fails with the following error message: "`Host Update Utility is unable to detect Cisco IMC firmware`"	4.0(2c)	4.0(2d)

Release 4.0(2c)

The following defects were resolved in release 4.0(2c):

Table 27: BMC

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvm12144	PSU input voltage lost assert issue seen though there is no physical power loss.	3.1(3b)	4.0(2c)
CSCvm27310	C-Series servers with NVIDIA P40 Card installed has fans running at 100% at all times. BMC sets the server to **Max Power** policy instead of **High Power** policy on the servers that have NVIDIA GPU P40 cards installed.	3.1(1d)	4.0(2c)
CSCvn04038	RAID cannot be set up between the two SD cards, resulting in the following error: `Controller State: Disconnected Partition From Host`	3.1(1d)	4.0(2c)

Table 28: CMC Storage

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvj95793	The "show fault-entries" list does not display the faults reported from the subordinate CMC when logged in using the management IP. It only reports the primary CMC faults.	4.0(1a)	4.0(2c)

Table 29: External Controllers

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvj74706	On the M4 servers, physical drives managed by UCSC-SAS12GHBA displays the physical drive state as **Unconfigured Good** instead of **JBOD**.	3.(3a)	4.0(2c)
CSCvm83587	On the C220 and 240 M5 servers with 3.1(3a) firmware versions, file transfer on VMware host results in Rx packet drops and CRC errors with Qlogic 25G card (QL41212H) running on driver version 8.21.x.	3.1(3a)	4.0(2c)

Table 30: Firmware Upgrade

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvk76542	Activation of Cisco UCS VIC cards or UCSC-C3260-SIOC card fails after upgrading to release 4.0(2c) or later. This happens on all C-Series Servers, and S3260 M5 servers that have these cards.	4.0(2c)	4.0(2c)

Table 31: Utilities

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvi65660	Cisco VIC adapter firmware may not automatically activate when you upgrade the firmware of the server components using the HUU. This happens when single server dual SIOC is enabled.	4.0(1a)	4.0(2c)

Open Caveats

The following section lists open caveats.

Open Caveats in Release 4.0(2)

Release 4.0(2c)

The following defects are open in release 4.0(2c):

Table 32: BIOS

Defect ID	Symptom	Workaround	First Affected Release
CSCvn09309	While trying to boot to PXE by pressing the **F12** key during POST, F12 network boot will not work for Cisco FastlinQ QL45611HLCU 100GBE adapter.	Press the **F6** or **F2** key and select Cisco FastlinQ QL45611HLCU 100GBE adapter for PXE boot.	4.0(2c)

Table 33: External Controllers

Defect ID	Symptom	Workaround	First Affected Release
CSCvm78123	ISCSI Boot protocol for Intel® XXV710-DA2 and X710-T4 cards is not displayed in the Boot Utility (bootutil) for the servers with firmware version 4.0(1a).	None	4.0(2c)

CSCvm78419	ISCSI lun may not be able establish TCP/IP connection with the Cisco Etherent Converged NIC X710-DA2, Intel X710-DA4 , and Intel XL710QDA2 PCIe cards after the firmware is updated to version 4.0(1a).	Use the following command on switch:
		`conf t`
		`    no lldp tlv-select dcbxp`
			4.0(2c)

Open Caveats in Release 4.0(1)

Release 4.0(1a)

The following defect is open in Release 4.0(1a):

Table 34: BIOS

Defect ID	Symptom	Workaround	First Affected Release
CSCvk58997	On the M4 servers, booting IPv6 based UEFI PXE using Windows WDS application fails with a server time out error. This happens with all M4 servers in UEFI mode.	Use IPv4 UEFI PXE.	4.0(1a)
CSCvo77732	After upgrading the C460 M4 servers with Intel® Xeon® Processor v2 to 4.0(1a) version, server encounters a CATERR fault and the server becomes unresponsive.	Downgrade to 3.0(x) version.	4.0(1a)

Table 35: VIC

Defect ID	Symptom	Workaround	First Affected Release
CSCvq64055	Cisco VIC1455 and VIC 1457 interfaces take more than four minutes to recover to Link-Up state after the far end Switch configuration is changed to no shut. This happens when a 25G 5M copper passive cable (SFP-H25G-CU5M) cable is connecting the VIC1455 or VIC 1457 and the N9K-C93180YC-EX switch.	Use shorter copper passive cables (SFP-25G-CU1M. SFP-25G-CU2M, SFP-25G-CU3M). Or Use optical cables.	4.0(1a)

Open Caveats in the Previous Releases

Refer to the following release notes for Open Caveats in the previous releases:

Release Notes for Cisco UCS C-Series Software

Known Behaviors

The following section lists known behaviors.

Known Behaviors in Release 4.0(2)

Release 4.0(2n)

The following caveats are known limitations in Release 4.0(2n):

Table 36: BIOS

Defect ID	Symptom	Workaround	First Affected Release
CSCvu62006	SLES15.2 and Ubuntu 20.04 OS successfully install on Cisco UCS C-Series and S-Series M4 servers with UEFI boot entry. However, booting to UEFI default boot entry deactivates after a reboot.	Perform the following steps: **1.** Enter BIOS setup and create an admin password. **2.** Go to **Advanced** > **Trusted Computing** and select **TCG_2** for TPM 1.2 or 2.0 UEFI version. **3.** Press **F10** to save and exit.	4.0(2m)

Release 4.0(2m)

The following caveats are known limitations in Release 4.0(2m):

Table 37: BMC

Defect ID	Symptom	Workaround	First Affected Release
CSCvm36382	Storage Controller on Cisco UCS S3260 M4 servers display `Invalid hardware configuration` error, after swapping the position from motherboard to IO Expander or from the IO Expander to the motherboard.	Run HUU on the server node after controller swap to update Sub OEMID to correct values.	4.0(2m)

Release 4.0(2c)

The following caveats are known limitations in Release 4.0(2c):

Table 38: BMC

Defect ID	Symptom	Workaround	First Affected Release
CSCvm08504	During a server firmware downgrade using the HUU, LLF (1050W PSUs) update fails when downgrading the firmware version from 4.0(1) to any previous releases.	None.	4.0(2c)

Table 39: External GPU Expander

Defect ID	Symptom	Workaround	First Affected Release
CSCvm92237	The **nvidia-smi** tool GPU slot mapping does not match with the **lspci** output and the C480-M5ML Silkscreen slot numbering.	To map **lspci** GPU slot **nr/BusID** to **nvidia-smi** GPU slot **nr/BusID**, run the following command (see the example below):	4.0(2c)

Mapping **lspci** GPU slot **nr/BusID** to **nvidia-smi** GPU slot **nr/BusID**:

```
[root@localhost ~]# lspci -tv

Search for Nvidia Devices with BusID 1b and 1c, for example;
the tree will display GPU PCI bridge BusID mapped to nvidia-smi GPU BusID:

lspci GPU PCI bridge BusID: 19:08.0 mapped with nvidia-smi GPU BusID: [1b]
(1B:00.0)
lspci GPU PCI bridge BusID: 19:0c.0 mapped with nvidia-smi GPU BusID: [1c]
(1C:00.0)

-[0000:17]-+-00.0-[18-1c]----00.0-[19-1c]--+-04.0-[1a]--
 |           |                               +-08.0-[1b]----00.0
                                   NVIDIA Corporation Device 1db5
 |           |                               \-0c.0-[1c]----00.0
                                  NVIDIA Corporation Device 1db5

To find a GPU slot nr, run the following command:

[root@localhost ~]# lspci -vvv -s 19:08.0 | grep -i slot
 Capabilities: [68] Express (v2) Downstream Port (Slot+), MSI 00
  LnkSta: Speed 8GT/s, Width x16, TrErr- Train-
              SlotClk- DLActive+ BWMgmt- ABWMgmt-
   Slot #3, PowerLimit 0.000W; Interlock- NoCompl-
  VC0: Caps: PATOffset=03 MaxTimeSlots=1 RejSnoopTrans-

[root@localhost ~]# lspci -vvv -s 19:0c.0 | grep -i slot
 Capabilities: [68] Express (v2) Downstream Port (Slot+), MSI 00
  LnkSta: Speed 8GT/s, Width x16, TrErr- Train- SlotClk-
             DLActive+ BWMgmt- ABWMgmt-
   Slot #4, PowerLimit 0.000W; Interlock- NoCompl-
  VC0: Caps: PATOffset=03 MaxTimeSlots=1 RejSnoopTrans-

lspci GPU Slot #3 (19:08.0) corresponds to nvidia-smi GPU Slot # 0 (1B:00.0)
lspci GPU Slot #4 (19:0c.0) corresponds to nvidia-smi GPU Slot # 1 (1C:00.0)

Repeat same steps for the other GPUs
```

Table 40: External OS

Defect ID	Symptom	Workaround	First Affected Release
CSCvj48637	HDD activity and locate LEDs are not working for AHCI controller. This happens when the Red Hat Enterprise Linux OS is installed.	None.	4.0(2c)
CSCvk15263	During installation, iSCSI LUN is not visible on Cavium OCP 41232 adapters with XEN 7.2, 7.3 or 7.4 OS versions.	None.	4.0(2c)

Known Behaviors in Release 4.0(1)

Release 4.0(1a)

The following caveat is a known limitation in Release 4.0(1a):

Table 41: CMC

Defect ID	Symptom	Workaround	First Affected Release
CSCvi46521	On the 3260 servers, when you are using a dual VIC single server configuration, you cannot access the second VIC.	You must enable the single server dual VIC feature to use the second VIC.	4.0(1a)

Table 42: External Controllers

Defect ID	Symptom	Workaround	First Affected Release
CSCvk11921	On the C125 servers with QL41232H 25G OCP card, the link does not work. This happens when OCP card is connected to the switch using a 5M SFP cable. The network LED is not on and the network is not functional.	1. Enter the BIOS setup. 2. Navigate to **Advanced** > **Qlogic QL41232 Option > Port Level configuration** 3. Change the link Speed to 25Gbps. 4. Press **F10**. 5. Save and exit.	4.0(1a)

Known Behaviors in the Previous Releases

Refer to the following release notes for Known Behaviors in the previous releases:

Release Notes for Cisco UCS C-Series Software

Related Documentation

Related Documentation

For configuration information for this release, refer to the following:

- Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide
- Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide
- Cisco UCS Rack-Mount Servers Cisco IMC API Programmer's Guide

For information about installation of the C-Series servers, refer to the following:

- Cisco UCS C-Series Rack Servers Install and Upgrade Guides

The following related documentation is available for the Cisco Unified Computing System:

- Cisco UCS C-Series Servers Documentation Roadmap
- Cisco UCS Site Preparation Guide
- Regulatory Compliance and Safety Information for Cisco UCS
- For information about supported firmware versions and supported UCS Manager versions for the rack servers that are integrated with the UCS Manager for management, refer to Release Bundle Contents for Cisco UCS Software.

Refer to the release notes for Cisco UCS Manager software and the *Cisco UCS C Series Server Integration with Cisco UCS Manager Guide* at the following locations:

- Cisco UCS Manager Release Notes
- Cisco UCS C Series Server Integration with Cisco UCS Manager Guides