Release Notes for Cisco UCS Rack Server Software, Release 4.1(3)

First Published: 2021-01-04

Last Modified: 2024-03-18

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 4.1(3) including Cisco Integrated Management Controller (Cisco IMC) software and any related BIOS, firmware, or drivers. Use this document in conjunction with the documents listed in the Related Documentation, on page 42 section.

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

Revision History

Revision	Date	Description
A4	March 18, 2024	Updated **New Software Features** for 4.1(3b).
H0	March 05, 2024	Created release notes for 4.1(3n). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.1.

Revision	Date	Description
G0	November 27, 2023	Created release notes for 4.1(3m). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.1.
F0	January 17, 2023	Created release notes for 4.1(3l). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.1.
E1	August 10, 2022	Updated **Known Behaviors and Limitations** for 4.1(3g).
G0	August 01, 2022	Created release notes for 4.1(3i). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.1.
F0	June 27, 2022	Created release notes for 4.1(3h). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.1.
E0	April 11, 2022	Created release notes for 4.1(3g). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.1.
D1	March 21, 2022	Updated Defect ID - CSCvz77885 for **Resolved Caveats in 4.1(3f)**.

Revision	Date	Description
D0	January 31, 2022	Created release notes for 4.1(3f). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.1.
A3	August 18, 2021	Updated New Hardware Support in Release 4.1(3b).
B1	August 03, 2021	Updated Resolved Caveats for 4.1(3c).
C0	July 30, 2021	Created release notes for 4.1(3d). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.1.
B0	May 31, 2021	Created release notes for 4.1(3c). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.1.
A2	March 30, 2021	Updated Resolved Caveats for 4.1(3b).
A1	February 01, 2021	Added Downgrade Limitation for Cisco UCS C125 M5 Servers.
A0	January 13, 2021	Created release notes for 4.1(3b). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.1.

Supported Platforms and Release Compatibility Matrix

Supported Platforms in this Release

The following Cisco UCS servers are supported in this release:

- UCS C125 M5
- UCS C220 M5
- UCS C240 SD M5
- UCS C240 M5
- UCS C480 M5
- UCS C480 ML M5
- UCS S3260 M5
- UCS S3260 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 4.1(3) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.1(3n)	NA	Cisco UCS C220 M5, C240 M5, C480 M5, S3260 M5 and S3260 M4 servers
4.1(3m)	4.1(3m)	Cisco UCS C220 M5, C240 M5, C480 M5, S3260 M5 and S3260 M4 servers
4.1(3l)	4.1(3k)	Cisco UCS C480 M5, C220 M5, C240 M5 servers
4.1(3i)	4.1(3j)	Cisco UCS C220 M5, C240 M5, C480 M5, S3260 M4, S3260 M5, C125 M5 servers
4.1(3h)	4.1(3i)	Cisco UCS C220 M5, C240 M5, C480 M5, S3260 M4, S3260 M5, C125 M5 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.1(3g)	No Support	Cisco UCS S3260 M4 and S3260 M5 servers
4.1(3f)	4.1(3h)	Cisco UCS C220 M5, C240 M5, C480 M5, S3260 M4, S3260 M4, S3260 M5, and C125 M5 servers
4.1(3d)	4.1(3e)	Cisco UCS C220 M5, C240 SD M5, C240 M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers
4.1(3c)	4.1(3d)	Cisco UCS C220 M5, C240 SD M5, C240 M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5 and C125 M5 servers
4.1(3b)	4.1(3a)	Cisco UCS C220 M5, C240 SD M5, C240 M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5 and C125 M5 servers

Table 2: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.1(2) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.1(2m)	No Support	Cisco UCS C220 M4, C240 M4 and C460 M4 servers.
4.1(2l)	No Support	Cisco UCS C220 M4 and C240 M4 servers.
4.1(2k)	No Support	Cisco UCS C220 M4, C240 M4, and C460 M4 servers
4.1(2j)	No Support	Cisco UCS C220 M4, C240 M4, and C460 M4 servers
4.1(2h)	No Support	Cisco UCS C220 M4, C240 M4, and C460 M4 servers
4.1(2g)	No Support	Cisco UCS C220 M4, C240 M4, and C460 M4 servers
4.1(2f)	4.1(2c)	Cisco UCS C220 M5, C240 SD M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.1(2e)	No Support	Cisco UCS C125 M5 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.1(2d)	No Support	Cisco UCS C240 M5 and C240 SD M5 servers
4.1(2b)	4.1(2b)	Cisco UCS C220 M5, C240 SD M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.1(2a)	4.1(2a)	Cisco UCS C220 M5, C240 SD M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers

Table 3: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.1(1) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.1(1h)	4.1(1e)	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
4.1(1g)	4.1(1d)	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
4.1(1f)	4.1(1c)	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
4.1(1d)	4.1(1b)	Cisco UCS C220 M5, C240 M5, C480 M5, and C480 ML M5 servers
4.1(1c)	4.1(1a)	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 4: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.0(4) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.0(4n)	4.0(4l)	Cisco UCS C220 M5, C240 M5, C480 M5, and S3260 M5 servers
4.0(4m)	4.0(4j)	Cisco UCS C220 M5, C240 M5, C480 M5, and S3260 M5 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.0(4l)	4.0(4i)	Cisco UCS C220 M5, C240 M5, C480 M5, and S3260 M5 servers
4.0(4k)	4.0(4h)	Cisco UCS C220 M5, C240 M5, and S3260 M5 servers
4.0(4j)	No Support	Cisco UCS S3260 M5 servers
4.0(4i)	4.0(4g)	Cisco UCS C220 M5, C240 M5, C480 M5 and S3260 M5 servers
4.0(4h)	4.0(4e)	Cisco UCS C220 M5, C240 M5, C480 M5 and S3260 M5 servers
4.0(4f)	4.0(4d)	Cisco UCS C220 M5, C240 M5, C480 M5, S3260 M5 and C480 ML M5 servers
4.0(4e)	4.0(4c)	Cisco UCS C220 M5, C240 M5, C480 M5, S3260 M5 and C480 ML M5 servers
4.0(4d)	No Support	Cisco UCS C220 M5, C240 M5, C480 M5 and S3260 M5 servers
4.0(4b)	4.0(4a)	Cisco UCS C220 M5, C240 M5, C480 M5, S3260 M5 and C480 ML M5 servers

Table 5: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.0(3) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.0(3b)	4.0(3a)	Cisco UCS C220 M5 and C240 M5 servers

Table 6: 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

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount 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 7: 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(1h)	No support.	Cisco UCS C220 M4, C240 M4, C460 M4, C220 M5, C240 M5, C480 M5 servers and C125 M5
4.0(1g)	No support.	Cisco UCS C220 M4, C240 M4, C460 M4, C220 M5, C480 M5 servers and C125 M5
4.0(1e)	No support.	Cisco UCS M4, M5 servers and C125 M5

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
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 8: 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 9: 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 10: 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 11: 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 12: 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 13: 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 14: 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

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 4.1(3):

- Microsoft Edge 87.0.664.47 or higher (64-bit)
- Google Chrome Version 87.0.4280.66 or higher (64-bit)
- Microsoft Internet Explorer 11.0.9600 or higher
- Mozilla Firefox 66.0.2 or higher (64-bit)
- Safari 14.0.1 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 4.1

The section provides information on the upgrade paths to release 4.1.

Important: While upgrading Cisco UCS C220 M5, C240 M5 or C480 M5 servers to release 4.1 under the following conditions:

- if you are upgrading from any release earlier than 4.0(4)
- if **Legacy Boot Mode** is enabled and no **Cisco IMC Boot Order** is configured
- and, if the server is booting from Cisco HWRAID adapter

then, you should perform one of the following before upgrading:

- Run XML-API scripts and UCSCFG based scripts provided at Configuring UCS Boot Order using the XML API.

  OR

- Manually configure the intended boot order through Cisco IMC GUI or CLI interfaces.

Refer to the table for upgrade paths for various Cisco UCS C-series IMC versions.

Table 15: Upgrade Paths to Release 4.1

Upgrade from Release	Upgrade to Release	Recommended Upgrade Path
All M5 servers from release 4.0	4.1	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 4.1(3b). • 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.
All M5 Servers from 3.1	4.1	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 4.1(3b). • 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)	4.1	Follow these steps to upgrade from releases greater than 3.0(3a) to 4.1(3b): • 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 4.1(3b). • 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)	4.1	Follow these steps to upgrade from releases less than 3.0(3a) to 4.1(3b): **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 4.1** • 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 4.1(3b). • 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

For details of Unified Computing System (UCS) Server Firmware, drivers, and utilities for release 4.1(3), seeCisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.1.

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 4.1.

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
- LSI Adapters
- LAN on Motherboard
- PCIe adapter firmware
- HDD firmware
- SAS Expander firmware
- DCPMM Memory

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

Note We recommend that you use the select all and **Update** or **Update & Activate 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:

http://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-rack-servers/products-user-guide-list.html

Downgrade Limitation

Downgrade Limitation for Cisco UCS C125 M5 Servers

Release 4.1(3b) introduces AMD Platform Secure Boot (PSB) in Cisco UCS C125 M5 servers that implements hardware-rooted boot integrity. Once you upgrade to release 4.1(3b) or later, you cannot:

- downgrade Cisco UCS C125 M5 Rack Server Node based on 2nd Gen AMD EPYC 7002 Series Processors (Rome) to any release earlier than 4.1(2e).
- downgrade Cisco UCS C125 M5 Rack Server Node based on AMD EPYC 7001 (Naples) to any release earlier than 4.0(2p).

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.

New Software Features in Release 4.1

New Software Features in Release 4.1(3d)

New BIOS token support for Cisco UCS C125 M5 servers:

- **Burst and Postponed Refresh** (default value - **Disabled**)

New Software Features in Release 4.1(3b)

For more information on new features, see Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide, Release 4.1 or Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Release 4.1.

The following new software features are supported in Release 4.1(3b):

- SNMP v3 users cannot be added with DES security protocol.
- Release 4.1(3b) 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.
- You can now disable only HTTP services from Cisco IMC.
- Support for TLS 1.3 communication
- Cisco IMC supports Hard Disk Drive (HDD) diagnostic self-test. You can monitor the drive health and performance using the diagnostic data obtained from the self-test.
- Cisco IMC supports Terminal Access Controller Access-Control System Plus (TACACS+) user authentication. You can configure up to six TACACS+ remote servers.
- You can configure **Minimum Security to Report** for each SMTP recipients.
- **COB Transmit Queue Count** now supports up to 64 SCSI I/O queues for 14xx series adapters and up to 245 queues for other adapters.
- Following BIOS tokens are introduced in this release:
    - Memory Thermal Throttling Mode
    - Panic and High Watermark
    - Memory Refresh Rate
- Cisco UCS M5 servers now support HTTP Boot capability that provides better performance over TFTP-based PXE methods for installing the OS. HTTP Boot capability can also be used to run EFI executable from remote HTTP server for diagnostics or configuration.
- Release 4.1(3b) introduces UEFI secure boot feature.

  Cisco UCS servers, running on Cisco IMC and BIOS firmware version 4.1(3b) or later, allow booting HUU 4.1(3b) or later in UEFI secure boot mode.

Intersight Management Mode

Intersight Managed Mode (IMM) is a new set of features introduced in Cisco Intersight to configure, deploy, and manage a Server Profile for C-Series FI-managed servers. IMM introduces a new implementation of concepts first introduced with Cisco IMC and moves ownership of the policy model into Cisco Intersight.

Cisco UCS Infrastructure and Server FW version 4.1(3) enables IMM; a policy driven configuration platform for FIs and attached servers. When IMM is enabled, the entire UCS domain is reset to factory defaults and this will cause a disruption for workloads running on servers in the domain.

New Hardware Features in Release 4.1

New Hardware Support in Release 4.1(3d)

The following new hardware are supported in Release 4.1(3d):

- Support for NVIDIA A-40 GPU on Cisco UCS C480 M5 servers.

New Hardware Support in Release 4.1(3b)

The following new hardware are supported in Release 4.1(3b):

- Support for NVIDIA A-100 GPU on Cisco UCS C240 M5 and C480 M5 servers.
- Support for 4 meter AOC cable connection from VIC 1455/57 at 25G to FI 6454 and N9300
- Support for Cisco Nexus K3P-S FPGA SmartNIC on Cisco UCS C240 M5 and C220 M5 servers.

Security Fixes

Security Fixes in Release 4.1(3m)

The following Security Fixes were added in Release 4.1(3m):

Defect ID - CSCwf30468

Cisco UCS C-Series M5 Rack Servers include an Intel® processor that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID(s):

- **CVE-2022-40982**—Information exposure through microarchitectural state after transient execution in certain vector execution units for some Intel® Processors may allow an authenticated user to potentially enable information disclosure through local access.
- **CVE-2022-43505**—Insufficient control flow management in the BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable denial of service through local access.

Defect ID - CSCwe96259

Cisco UCS C-Series Rack Servers are affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID(s):

- **CVE-2023-20228**—A vulnerability in the web-based management interface of Cisco IMC could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the browser of the targeted user or access sensitive, browser-based information.

Defect ID - CSCwf98321

Cisco UCS S-Series S3260 M4 Rack Servers are affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID(s):

- **CVE-2022-38083**—Improper initialization in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable information disclosure through local access.
- **CVE-2022-43505**—Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable denial of service through local access.

Security Fixes in Release 4.1(3i)

The following Security Fix was added in Release 4.1(3i):

Defect ID - CSCwb67159

Cisco UCS C-Series M5 Rack Servers include an Intel® processor that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID(s):

- **CVE-2021-0189**—Use of out-of-range pointer offset in the BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable escalation of privilege through local access.
- **CVE-2021-0159**—Improper input validation in the BIOS authenticated code module for some Intel® Processors may allow a privileged user to potentially enable escalation of privilege through local access.
- **CVE-2021-33123**—Improper access control in the BIOS authenticated code module for some Intel® Processors may allow a privileged user to potentially enable escalation of privilege through local access.
- **CVE-2021-33124**—Out-of-bounds write in the BIOS authenticated code module for some Intel® Processors may allow a privileged user to potentially enable escalation of privilege through local access.
- **CVE-2022-21131**—Improper access control for some Intel® Xeon® Processors may allow an authenticated user to potentially enable information disclosure through local access.
- **CVE-2022-21136**—Improper input validation for some Intel® Xeon® Processors may allow a privileged user to potentially enable denial of service through local access.

Security Fixes in Release 4.1(3h)

The following Security Fix was added in Release 4.1(3h):

Defect ID - CSCwb67159

Cisco UCS M5 servers, based on Intel® Processors are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- **CVE-2021-0154**—Improper input validation in the BIOS firmware for some Intel® Processors may allow a privileged user to enable escalation of privilege through local access.
- **CVE-2021-0155**—Unchecked return value in the BIOS firmware for some Intel® Processors might allow a privileged user to enable information disclosure through local access.

- **CVE-2021-0189**—Use of out-of-range pointer offset in the BIOS firmware for some Intel® Processors might allow a privileged user to enable escalation of privilege through local access.
- **CVE-2021-33123**—Improper access control in the BIOS authenticated code module for some Intel® Processors might allow a privileged user to enable escalation of privilege through local access.
- **CVE-2021-33124**—Out-of-bounds write in the BIOS authenticated code module for some Intel® Processors might allow a privileged user to enable escalation of privilege through local access.

Security Fixes in Release 4.1(3f)

The following Security Fixes were added in Release 4.1(3f):

Defect ID - CSCvy91321

Cisco Integrated Management Controller (IMC) Software are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- **CVE-2021-34736**—A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to cause the web-based management interface to unexpectedly restart.

  The vulnerability is due to insufficient input validation on the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause the interface to restart, resulting in a denial of service (DoS) condition.

  Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

Defect ID - CSCvz48566

Cisco UCS C220 M4 and M5 servers are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- **CVE-2021-3712**—ASN.1 strings are represented internally within OpenSSL as an ASN1_STRING structure, which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are represented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own **d2i** functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1_STRING_set() function will additionally NUL terminate the byte array in the ASN1_STRING structure.

  However, it is possible for applications to directly construct valid ASN1_STRING structures which do not NUL terminate the byte array by directly setting the "data" and "length" fields in the ASN1_STRING array. This can also happen by using the ASN1_STRING_set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to assume that the ASN1_STRING byte array will be NUL terminated, even though this is not guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be printed, and where that ASN.1 structure contains ASN1_STRINGs that have been directly constructed by the application without NUL terminating the **data** field, then a read buffer overrun can occur.

  The same thing can also occur during name constraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1_STRING structures). It can also occur in the X509_get1_email(), X509_REQ_get1_email() and X509_get1_ocsp() functions.

An attacker can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack). It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext).

This release includes SSL revisions for Cisco UCS M4 and M5 rack servers. These revisions include update for rack servers, which is a required part of the mitigation for these vulnerabilities.

Defect ID - CSCvz48570

Cisco UCS C220 M4 and M5 servers are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- **CVE-2021-3711**—Implementation of the SM2 decryption code that can lead to a buffer overflow when calling the API function to decrypt SM2 encrypted data. An attacker presenting a specially crafted SM2 content may be able to exploit the vulnerability and change application behavior or cause the application to crash. An attacker exploiting the vulnerability may be able to disclose private memory contents or perform a Denial of Service (DoS) attack.

This release includes SSL revisions for Cisco UCS M4 and M5 rack servers. These revisions include update for rack servers, which is a required part of the mitigation for these vulnerabilities.

Security Fixes in Release 4.1(3d)

The following Security Fixes were added in Release 4.1(3d):

Defect ID - CSCvy16762

Cisco UCS C-Series and S-Series M5 servers, based on Intel® Processors are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- **CVE-2020-12358**—Out of bounds write in the firmware for some Intel® Processors may allow a privileged user to enable denial of service through local access.
- **CVE-2020-12360**—Out of bounds read in the firmware for some Intel® Processors may allow an authenticated user to enable escalation of privilege through local access.
- **CVE-2020-24486**—Improper input validation in the firmware for some Intel® Processors may allow an authenticated user to enable denial of service through local access.
- **CVE-2020-24511**—Improper isolation of shared resources in some Intel® Processors may allow an authenticated user to enable information disclosure through local access.

This release includes BIOS revisions for Cisco UCS M5 rack servers. These BIOS revisions include Microcode update for Cisco UCS M5 rack servers, which is a required part of the mitigation for these vulnerabilities.

Security Fixes in Release 4.1(3c)

The following Security Fixes were added in Release 4.1(3c):

Defect ID - CSCvx82648

Cisco UCS C-Series and S-Series M5 servers, based on Intel® Processors are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- **CVE-2021-3449**—may allow a remote unauthenticated user to crash a TLS server resulting in a Denial of Service (DoS) condition.
- **CVE-2021-3450**—may allow a remote unauthenticated user to conduct a MiTM attack or to impersonate another user or device by providing a crafted certificate.

Security Fixes in Release 4.1(3b)

The following Security Fixes were added in Release 4.1(3b):

Defect ID - CSCvv34145

Cisco UCS C-Series and S-Series M5 servers, based on Intel® Processors are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- **CVE-2020-0587**—Improper conditions check in BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable escalation of privilege through local access.
- **CVE-2020-0588**—Improper conditions check in BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable escalation of privilege through local access.
- **CVE-2020-0590**—Improper input validation in BIOS firmware for some Intel® Processors may allow an authenticated user to potentially enable escalation of privilege through local access.
- **CVE-2020-0591**—Improper buffer restrictions in BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable escalation of privilege through local access.
- **CVE-2020-0592**—Out of bounds write in BIOS firmware for some Intel® Processors may allow an authenticated user to potentially enable escalation of privilege and/or denial of service through local access.
- **CVE-2020-0593**—Improper buffer restrictions in BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable escalation of privilege through local access.
- **CVE-2020-8696**—Improper removal of sensitive information before storage or transfer in some Intel® Processors may allow an authenticated user to potentially enable information disclosure through local access.
- **CVE-2020-8698**—Improper isolation of shared resources in some Intel® Processors may allow an authenticated user to potentially enable information disclosure through local access.
- **CVE-2020-8705**—Insecure default initialization of resource in Intel® Boot Guard in Intel® CSME versions before 11.8.80, 11.12.80, 11.22.80, 12.0.70, 13.0.40, 13.30.10, 14.0.45 and 14.5.25, Intel® TXE versions before 3.1.80 and 4.0.30, Intel(R) SPS versions before E5_04.01.04.400, E3_04.01.04.200, SoC-X_04.00.04.200 and SoC-A_04.00.04.300 may allow an unauthenticated user to potentially enable escalation of privileges through physical access.
- **CVE-2020-8755**—Race condition in subsystem for Intel® CSME versions before 12.0.70 and 14.0.45, Intel® SPS versions before E5_04.01.04.400 and E3_05.01.04.200 may allow an unauthenticated user to potentially enable escalation of privilege through physical access.

- **CVE-2020-8738**—Improper conditions check in Intel® BIOS platform sample code for some Intel® Processors before may allow a privileged user to potentially enable escalation of privilege through local access.
- **CVE-2020-8739**—Use of potentially dangerous function in Intel BIOS platform sample code for some Intel® Processors may allow an authenticated user to potentially enable escalation of privilege through local access.
- **CVE-2020-8740**—Out of bounds write in Intel BIOS platform sample code for some Intel® Processors may allow a privileged user to potentially enable escalation of privilege through local access.
- **CVE-2020-8764**—Improper access control in BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable escalation of privilege through local access.

Resolved Caveats

Resolved Caveats in 4.1(3n)

The following caveats were resolved in Release 4.1(3n):

Defect ID	Symptom	First Release Affected	Resolve in Release
CSCwj00617	In Cisco UCS M5 servers, the SAS expander firmware update from the XML API interface, using HTTP and TFTP protocol, fails and displays the following error message: Operation failed. Invalid Password! This issue is now resolved.	4.2(3i)	4.1(3n)
CSCwi97945	In Cisco UCS M5 servers, the SAS expander firmware update from the CLI interface, using HTTP and TFTP protocol, fails and displays the following error message: Operation failed. Invalid Password! This issue is now resolved.	4.2(3i)	4.1(3n)

Resolved Caveats in 4.1(3m)

The following caveats were resolved in Release 4.1(3m):

Defect ID	Symptom	First Release Affected	Resolve in Release
CSCwb82433	Cisco UCS C220 M5 servers, equipped with Cisco UCS VIC 1400 series adapter and have Geneve enabled, go offline after the Cisco UCS VIC adapters fail to respond. This issue is now resolved.	4.1(3d)	4.1(3m)
CSCwe35644	Several ECCs are observed on a single DIMM with no fault from Cisco UCS Manager in Cisco UCS C-Series M5 and M6 servers equipped with 64GB DIMMs (UCS-MR-X64G2RW) and ADDDC enabled. This issue is now resolved.	4.1(3e)	4.1(3m)

Resolved Caveats in 4.1(3l)

The following defects were resolved in Release 4.1(3l):

Table 16: BMC

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwd20131	In Cisco UCS C480 M5 servers, the BIOS tokens are not displayed for the following adopter PID: • DN2-HW-APL-XL-U However, the BIOS tokens are displayed for the following adopter PID: • DN2-HW-APL-XL This issue is now resolved.	4.1(3d)	4.1(3l)

Table 17: BIOS-EX

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwd04797	Cisco UCS M5 servers equipped with NVMe drives get stuck at POST in legacy boot mode after UCS firmware upgrade. This issue is resolved.	4.1(3h)	4.1(3l)

Resolved Caveats in 4.1(3h)

The following caveats were resolved in Release 4.1(3h):

Table 18: BMC

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwa85667	BMC reset is observed on Cisco UCS C-Series M5/M6 servers due to kernel crash and watchdog reset. This issue is now resolved.	4.0(4m)	4.2(1a)
CSCwb33753	During IMM deployment, auto-update of the device connector on a server might fail with the following error message: `Stderr: mount: can't setup loop device: No such file or directory` This issue is now resolved.	4.1(3f)	4.2(1i)

Table 19: Firmware Upgrade

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwb21128	Under certain conditions, the hard drive might experience long latency times, leading to undesirable results while working with latency-sensitive applications. This issue might happen with small block size and sequential writes. This issue is now resolved.	4.1(3c)	4.1(3g)

Resolved Caveats in 4.1(3g)

The following caveats were resolved in Release 4.1(3g):

Table 20: Firmware Upgrade

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwa98283	Server reboots into the host upgrade utility instead of the correct target device during the Intersight upgrade of the server. This issue is now resolved.	4.1(3c)	4.1(3g)
CSCwb21128	Under certain conditions, the hard drive might experience long latency times, leading to undesirable results while working with latency-sensitive applications. This issue might happen with small block size and sequential writes. This issue is now resolved.	4.1(3c)	4.1(3g)

Resolved Caveats in 4.1(3f)

The following caveats were resolved in Release 4.1(3f):

Table 21: BMC

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvz29291	Attempting to mount an ISO on a Cisco UCS C-Series server using the Cisco APIs through HTTP or HTTPS results in a failure and the following error message: `Local Device Mount Failed was displayed.` This issue is now resolved.	4.1(3b)	4.1(3f)
CSCvz76449	In Cisco UCS C-Series M5 servers, while creating a service profile using Intersight, you may be unable to apply a profile which has two RoCE vNics and two VMQ/VMMQ vNics. Following error message is displayed: `The adapter cannot have more than 2 rdma profiles configured` This issue is now resolved.	4.1(3c)	4.1(3f)

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvz73890	Cisco UCS C-Series M5 servers do not show up in the list in Intersight. The following message is also displayed: `The current operation failed. CIMC may be running any critical operation or in error state. Retry after sometime or reboot CIMC if necessary` This issue is now resolved.	4.1(2b)	4.1(3f)
CSCvy78034	Redfish API displays incorrect CPU thread count. This issue is now resolved.	4.1(3b)	4.1(3f)
CSCvz77885	In Cisco UCS C-Series M5 servers, Cisco IMC reboots unexpectedly due to Watchdog service reset. This issue is now resolved.	4.1(3d)	4.1(3f)

Table 22: BMC Storage

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvy11359	Cisco UCS HX-M5 rack servers integrated with Cisco UCS Manager do not contain SAS Expander tech support information. This issue is now resolved.	4.1(3d)	4.1(3f)

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvy74166	In Cisco UCS C-Series M4 rack servers, after enabling encryption through HX Connect, HX Connect shows status as **Partially Encrypted**, whereas Cisco UCS Manager and HX CLI display encryption enabled as expected. This issue is now resolved.	4.1(2b)	4.1(3f)

Table 23: BIOS

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvz36957	Server UUID set in the Server Profile of a Cisco UCS C-Series server is not displayed under the server inventory page. This issue is now resolved.	4.1(3d)	4.1(3f)

Table 24: Firmware Upgrade

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvy75787	In Cisco UCS C240 M5 servers equipped with Emulex LPe32002 Dual-port 32G FC HBA, link status for one of the links goes into **Bypassed** state. This issue is now resolved.	4.1(2d)	4.1(3f)

Table 25: FlexFlash

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvz49944	After power cycling Cisco UCS C125 M5 servers, it is unable to detect the SD card, and hence is unable to boot as the boot device is unreachable. This issue is now resolved.	4.1(3c)	4.1(3f)

Table 26: Host Firmware Upgrade

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvz95318	When the configuration of port 1 and 2 are identical on a Qlogic card, port 1 disconnects whenever the server reboots. This issue is now resolved.	4.1(3c)	4.1(3f)

Resolved Caveats in 4.1(3d)

The following caveats were resolved in Release 4.1(3d):

Table 27: BMC

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvy50012	In Cisco C220 M5 servers, Redfish API displays error while configuring NTP servers while using IPv6 address. This issue is now resolved.	4.1(3b)	4.1(3d)
CSCvy87338	Deleting or Terminating a Redfish sessions using the **logout()** method from the Redfish Python library fails with HTTP response code 404 error. This issue is now resolved.	4.1(3c)	4.1(3d)

Table 28: SNMP

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvy51599	In Cisco UCS C-Series M5 servers running Cisco IMC version 4.1(3b) or later, SNMP services restart frequently when **snmpbulkget** with higher **Cr** value is triggered against Cisco IMC. This issue is now resolved.	4.1(3c)	4.1(3d)

Resolved Caveats in 4.1(3c)

The following caveats were resolved in Release 4.1(3c):

Table 29: BMC

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvw51939	Cisco IMC may reset abruptly in Cisco UCS C-Series M5 servers during normal operation. This issue is now resolved.	4.1(2b)	4.1(3c)
CSCvy26376	Cisco IMC mail alert fails on Cisco UCS C-Series C220 M5 servers and no email is sent when a fault is generated. This issue is now resolved.	4.1(3b)	4.1(3c)
CSCvx65636	Cisco IMC CLI commands for debugging LDAP authentication do not display any result. This issue is now resolved.	4.1(3b)	4.1(3c)

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvw57963	Intersight Hardware Compatibility list incorrectly displays driver version compliance issues for up to date servers. This issue is now resolved.	4.1(2b)	4.1(3c)

Table 30: CMC

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvw38535	In Cisco UCS S3260 M5 servers, both SASEXP are reset due to heartbeat loss with CMC. This issue is now resolved.	4.0(4f)	4.1(3c)

Table 31: External PSU

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvx04641	In Cisco UCS M5 servers, PSU reports unexpected high input power to BMC when server runs on Aux power mode (server powered off). BMC reports this on SEL log. This issue is now resolved.	4.0(1a)	4.1(3c)

Table 32: Host Firmware Upgrade

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvu63139	In Cisco UCS C240 M5 stand alone servers when Qlogic cards are connected to FC LUN, HUU does not respond while booting. This issue is now resolved.	4.0(1c)	4.1(3c)

Table 33: SNMP

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvx03201	In Cisco UCS C240 M5 servers, SNMP displays incorrect over all server status when one PSU is removed. This issue is now resolved.	4.0(4b)	4.1(3c)

Table 34: XML API

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvx42679	Following error is displayed while using XML API for Cisco UCS C220 M5 servers to set a hostname configuration on NTP LDAP: `is not a valid value of the union type emptyStringOrHostNameOrIPv4AddressOrIPv6Address` This issue is now resolved.	4.0(4m)	4.1(3c)

Resolved Caveats in 4.1(3b)

The following caveats were resolved in Release 4.1(3b):

Table 35: BIOS

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvw43093	NIHUU update times out in Cisco UCS C125 server nodes when Cisco IMC update is in progress for a long time and does not proceed. This issue is resolved.	4.1(3b)	4.1(3b)

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvw49192	After upgrading to release 4.1(2b), some system configurations may be unable to perform power characterization resulting in a POST failure. System freezes at **Loading PTU driver** screen. CATERR is also logged in the SEL. This issue is now resolved.	4.1(2b)	4.1(2f) and 4.1(3b)

Table 36: BMC

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvp35008	SLES/RHEL OS installation in UEFI mode fails on Cisco UCS C-Series M5 servers when they are equipped with Intel Xx710 adapters, and one or more of these adapters has the Option ROM enabled. This issue is now resolved.	4.0(4b)	4.0(4l) and 4.1(3b)
CSCvv97789	Cisco UCS M4 servers fail to accept the default admin password in F8 boot utility under the following conditions: • servers are running release 4.1(1c) or 4.1(2a) • servers are reset to factory default settings for any reason Due to this, you cannot use the F8 configuration utility. This issue is now resolved.	4.1(2a)	4.1(3b)

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvv08053	Cisco UCS C-Series M4 and earlier model servers, in UCS Manager attached mode—if two IP addresses are configured in Inband mode from the same VLAN ID, then only one IP address is assigned after a fabric failover. This issue is now resolved.	4.1(2a)	4.1(3b)
CSCvi46928	Cisco IMC reboots without any reason in Cisco UCS C480 servers. Cisco IMC logs do not show any error or Out of Memory issues. This issue is now resolved.	3.1(2b)	4.1(3b)

Table 37: External Controllers

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvq53066	Upgrading host firmware from release 4.0(2x) or earlier to release 4.0(4b) or later using auto-install in a Cisco UCS C240 M5 server, results in SAS controller firmware activation failure. Following faults are seen: • F78413 - Update Failed on Storage Controller • F0181 - Drive state: unconfigured bad • F0856 - Activation failed and Activate Status set to failed This issue is now resolved.	4.0(4d)	4.0(4l), 4.1(1g), and 4.1(3b)

Open Caveats

Open Caveats in Release 4.1(3c)

The following defects are open in Release 4.1(3c):

Table 38:

Defect ID	Symptom	Workaround	First Affected Release
CSCvy51599	In Cisco UCS C-Series M5 servers running Cisco IMC version 4.1(3b) or later, SNMP services restart frequently when **snmpbulkget** with higher **Cr** value is triggered against Cisco IMC.	Restart Cisco IMC.	4.1(3b)

Open Caveats in Release 4.1(3b)

The following defects are open in Release 4.1(3b):

Table 39: BMC

Defect ID	Symptom	Workaround	First Affected Release
CSCvv10194	Cisco IMC Web GUI is inaccessible when: • TLS 1.3 communication is enabled and TLS 1.2 communication is disabled in the web browser. • **Common Criteria mode** is enabled in Cisco IMC.	Enable TLS 1.2 communication in the web browser.	4.1(3b)

Table 40: External Controllers

Defect ID	Symptom	Workaround	First Affected Release
CSCvr49058	Intel x520 iSCSI LUN is not detected during POST in Cisco UCS M5 servers under the following conditions: • iSCSI boot is configured on Intel x520 adapter • Intel x520 adapter is running firmware version 0x800008A4-1.817.3 or higher Boot mode is set to UEFI.	Downgrade Intel x520 adapter firmware version to 0x800008A4-1.812.1	4.1(3b)

Table 41: Host Firmware Upgrade

Defect ID	Symptom	Workaround	First Affected Release
CSCvw68180	In Cisco UCS S-series server, NIHUU fails to upgrade to release 4.1(3b) due to ISO mapping error. This issue occurs under the following conditions: • ISO mapping share is configured as CIFS • **mountOption** parameter is specified in NIHUU configuration file.	Perform one of the following workarounds: **1.** Use NFS share for ISO mapping. **2.** Use HTTP/HTTPS share for ISO mapping. **3.** Use CIFS share which does not need any **mountOption** parameter for ISO mapping. **4.** Update and activate Cisco IMC firmware using XML API. **5.** Update and activate Cisco IMC firmware using Cisco IMC Web GUI.	4.1(3b)

Known Behaviors and Limitations

Known Behaviors and Limitations in Release 4.1(3g)

The following caveat is a known limitation in release 4.1(3g):

Table 42: BMC Storage

Defect ID	Symptom	Workaround	First Affected Release
CSCwc64817	In Cisco UCS S3260 M5 servers running Cisco IMC release 4.1(3g): Redfish API user interface does not populate the drive list under **SimpleStorage** resource.	Use the resources under **Storage** resource. The resources under **SimpleStorage** resource are deprecated.	4.1(3g)

Known Behaviors and Limitations in Release 4.1(3d)

The following caveats are known limitations in release 4.1(3d):

Table 43: BMC

Defect ID	Symptom	Workaround	First Affected Release
CSCvy34100	In Cisco UCS S3260 M4 servers running Cisco IMC release 4.1(3x) and having saved VMedia mapping, the following issue is observed: The saved VMedia mappings are not visible when Cisco IMC is downgraded to release 4.1(2a) or earlier. User is unable to map new VMedia using Cisco IMC GUI.	Perform the following steps to clear the saved VMEDIA mapping using Cisco IMC CLI. **1.** UCS# scope server *n* **2.** UCS /server # scope vmedia **3.** UCS /server/vmedia # delete-saved-mappings **4.** Enter `yes` to confirm. Once cleared, the VMedia mapping works as expected from all interfaces (GUI, CLI, and XML API).	4.1(3c)

Known Behaviors and Limitations in Release 4.1(3b)

The following caveats are known limitations in release 4.1(3b):

Table 44: BIOS

Defect ID	Symptom	Workaround	First Affected Release
CSCvu62006	SLES 15.2 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)

Table 45: BMC

Defect ID	Symptom	Workaround	First Affected Release
CSCvu99928	Old SSH client fails to connect to Cisco IMC when FIPS is enabled.	Upgrade SSH client version or disable FIPS in Cisco IMC.	4.1(3b)

Table 46: External Controller

Defect ID	Symptom	Workaround	First Affected Release
CSCvw22319	VMD with HGST NVME drives is not supported on Cisco UCS C480 M5 servers	Disable VMD when HGST drives are used in Cisco UCS C480 M5 servers.	4.1(3b)
CSCvo39645	CATERR/IERR occurs on multiple concurrent reboots and the system becomes unresponsive during POST. This issue occurs on servers with NVMe drives on mSwitch connected configuration.	Perform a warm reboot.	4.0(4b)
CSCvs30287	Multiple critical SEL events are observed in Cisco UCS C125 servers based on AMD EPYC 7352 (ROME) processors, equipped with HGST NVMe drives	Reboot the server.	4.1(2a)

Table 47: Operating System

Defect ID	Symptom	Workaround	First Affected Release
CSCvu80469	Installation of mpt3sas driver fails after installing i40e drivers on SLES 12.5 OS in Cisco UCS servers equipped with Intel 710 series adapters and pass through HBA controller. Following warning message is displayed: `Updating / installing... 1:lsi-mpt3sas-kmp-default-30.00.01.# [100%]depmod: WARNING: //lib/modules/4.12.14-119-default/kernel/drivers/infiniband/hw/i40iw/i40iw.ko disagrees about version of symbol i40e_unregister_client depmod: WARNING: //lib/modules/4.12.14-119-default/kernel/drivers/infiniband/hw/i40iw/i40iw.ko disagrees about version of symbol i40e_register_client Warning: /lib/modules/4.12.14-119-default is inconsistent Warning: weak-updates symlinks might not be created`	Perform one of the following: **1.** Uninstall i40e driver **2.** Change the order of installation. Install mpt3sas driver first and then i40e driver.	4.1(2a)

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