Release Notes for Cisco UCS Rack Server Software, Release 4.2(2)

First Published: 2022-07-08

Last Modified: 2023-01-10

Cisco UCS C-Series Servers

Cisco UCS C-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 software release 4.2(2) 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 37 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
C1	January 10, 2023	Updated the section **Resolved Caveats in 4.2(2g)**

Revision	Date	Description
C0	November 23, 2022	Created release notes for 4.2(2g) for the following servers: Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.2
B2	October 31, 2022	Updated the section **New Hardware in Release 4.2(2f)**.
A5	October 31, 2022	Updated the section **New Hardware in Release 4.2(2a)**.
A4	October 18, 2022	Updated the section **New Software Features in Release 4.2(2a)**
A3	October 10, 2022	Updated the section **New Hardware in Release 4.2(2a)**.
B0	September 20, 2022	Created release notes for 4.2(2f) for the following servers: Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.2
A2	August 10, 2022	Added CSCwc64817 in **Known Behaviors and Limitations**.
A1	July 28, 2022	Updated **Upgrade Paths to Release 4.2**.

Revision	Date	Description
A0	July 8, 2022	Created release notes for 4.2(2a) for the following servers: Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.2

Supported Platforms and Release Compatibility Matrix

Supported Platforms in this Release

The following servers are supported in this release:

- Cisco UCS C220 M6
- Cisco UCS C240 M6
- Cisco UCS C245 M6
- Cisco UCS C225 M6
- Cisco UCS C220 M5
- Cisco UCS C240 M5
- Cisco UCS C240 SD M5
- Cisco UCS C480 M5
- Cisco UCS S3260 M5
- Cisco UCS C480 M5
- Cisco UCS C480 M5 ML
- Cisco UCS C125 M5
- Cisco 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 Rack-Mount Servers are managed by built-in standalone software —Cisco IMC. However, when a Rack-Mount Server is integrated with Cisco UCS Manager, UCSM end-user interface is used to manage the server.

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 4.2(2) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.2(2g)	4.2(2d)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers
4.2(2f)	4.2(2c)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers
4.2(2a)	4.2(2a)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD 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 4.2(1) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.2(1j)	4.2(1n)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers
4.2(1i)	4.2(1m)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers
4.2(1g)	No Support	Cisco UCS C225 M6 and C245 M6 servers
4.2(1f)	4.2(1k)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers
4.2(1e)	4.2(1i)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.2(1c)	No Support	Cisco UCS C225 M6 and C245 M6 servers
4.2(1b)	4.2(1f)	Cisco UCS C220 M6 and C240 M6 servers
4.2(1a)	4.2(1d)	Cisco UCS C220 M6, C240 M6, and C245 M6 servers

Table 3: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.2(1) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.2(1j)	4.2(1n)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers
4.2(1i)	4.2(1m)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers
4.2(1g)	No Support	Cisco UCS C225 M6 and C245 M6 servers
4.2(1f)	4.2(1k)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers
4.2(1e)	4.2(1i)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers
4.2(1c)	No Support	Cisco UCS C225 M6 and C245 M6 servers
4.2(1b)	4.2(1f)	Cisco UCS C220 M6 and C240 M6 servers
4.2(1a)	4.2(1d)	Cisco UCS C220 M6, C240 M6, and C245 M6 servers

Table 4: 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(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 5: 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(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
4.1(2d)	No Support	Cisco UCS C240 M5 and C240 SD M5 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount 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 6: 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 7: 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
4.0(4l)	4.0(4i)	Cisco UCS C220 M5, C240 M5, C480 M5, and S3260 M5 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount 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 8: 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 9: 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 10: 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 11: 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 12: 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 13: 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 14: 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 15: 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 16: 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 17: 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 4.2(2):

Recommended Browser	Browser Version	Recommended Operating System
Microsoft Edge	95.0.1020.53(Official Build) (64-bit)	Microsoft Windows 10 x64
	98.0.1108.50 (Official build) (64-bit)	Microsoft Windows 10 x64
Google Chrome	96.0.4664.45	
	96.0.4664.45 (Official Build) (64-bit)	
	94.0.4606.71 (Official Build) (64-bit)	
Mozilla Firefox	94.0.2 Build ID: 20211119140621	MAC Monterey v.12.0.1
	97.0.1	Microsoft Windows 10 x64
	78.9.0 ESR (64-bit)	RHEL 8.4

Recommended Browser	Browser Version	Recommended Operating System
Safari	14.1.2 (16611.3.10.1.6)	MAC Monterey v.12.0.1
	15.1 (17612.2.9.1.20)	

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 Cisco Optics-to-Device Compatibility Matrix

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

Default Ports

Following is a list of server ports and their default port numbers:

Table 18: Server Ports

Port Name	Port Number
LDAP Port 1	389
LDAP Port 2	389
LDAP Port 3	389
LDAP Port 4	3268
LDAP Port 5	3268
LDAP Port 6	3268
SSH Port	22

Port Name	Port Number
HTTP Port	80
HTTPS Port	443
SMTP Port	25
KVM Port	2068
Intersight Management Port	8889
Intersight Cloud Port	8888
SOL SSH Port	2400
SNMP Port	161
SNMP Traps	162
External Syslog	514

Upgrade Paths to Release 4.2

The section provides information on the upgrade paths to release 4.2.

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

Table 19: Upgrade Paths to Release 4.2(2x)

Upgrade From Release	Upgrade To Release	Recommended Upgrade Path
4.2(2a)	• 4.2(2g) • 4.2(2f)	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 4.2(2a). • 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
All Cisco UCS M6 Servers from 4.2(1a)	• 4.2(2g) • 4.2(2f) • 4.2(2a)	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 4.2(1a). • 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.
Following Cisco UCS Servers from 4.1(3): • Cisco UCS C220 M5 • Cisco UCS C240 M5 • Cisco UCS C240 SD M5 • Cisco UCS C480 M5 • Cisco UCS C480 M5 ML • Cisco UCS S3260 M5 • Cisco UCS C125 M5 • Cisco UCS S3260 M4	• 4.2(2f) • 4.2(2a)	Follow below upgrade path: • 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(3). • 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
Following Cisco UCS Servers from 4.1(2): • Cisco UCS C220 M5 • Cisco UCS C240 M5 • Cisco UCS C240 SD M5 • Cisco UCS C480 M5 • Cisco UCS C480 M5 ML • Cisco UCS S3260 M5 • Cisco UCS C125 M5 • Cisco UCS S3260 M4	• 4.2(2f) • 4.2(2a)	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(2). • 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.
Following Cisco UCS Servers from 4.1(1): • Cisco UCS C220 M5 • Cisco UCS C240 M5 • Cisco UCS C480 M5 • Cisco UCS C480 M5 ML • Cisco UCS S3260 M5 • Cisco UCS C125 M5 • Cisco UCS S3260 M4	• 4.2(2f) • 4.2(2a)	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(1). • 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.
Following Cisco UCS Servers from 4.0(4): • Cisco UCS C220 M5 • Cisco UCS C240 M5 • Cisco UCS C480 M5 • Cisco UCS C480 M5 ML • Cisco UCS S3260 M4	• 4.2(2f) • 4.2(2a)	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(4). • 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.

Refer to the table for upgrade options from Cisco IMC 4.2(1a) release:

Table 20: Upgrade Paths to Release 4.2(1a)

Server	Upgrade from Release	Upgrade to Release
Cisco UCS C220 M6	4.2(1a)	4.2(1b), 4.2(1e), and 4.2(1f)
Cisco UCS C240 M6	4.2(1a)	4.2(1b), 4.2(1e), and 4.2(1f)
Cisco UCS C245 M6	4.2(1a)	4.2(1g), 4.2(1c), 4.2(1e), 4.2(1f), and 4.2(1g)
Cisco UCS C225 M6	4.2(1c)	4.2(1e), 4.2(1f), and 4.2(1g)

Firmware Upgrade Details

Firmware Files

The C-Series software release 4.2(2) includes the following software files:

CCO Software Type	File name(s)	Comment
Unified Computing System (UCS) Server Firmware	For release specific ISO versions, see Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.2	Host Upgrade Utility
Unified Computing System (UCS) Drivers	ucs-cxxx-drivers.4.2.2a.iso	Drivers
Unified Computing System (UCS) Utilities	ucs-cxxx-utils-efi.4.2.2a.iso ucs-cxxx-utils-linux.4.2.2a.iso ucs-cxxx-utils-vmware.4.2.2a.iso ucs-cxxx-utils-windows.4.2.2a.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 4.2.

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
- Storage controller firmware

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

Note We recommend that you use **Update & Activate** 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. To force update the component, toggle **Advance mode** and select the required firmware component and click **Update & Activate**. Click **Power Cycle** icon 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

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 4.2

New Software Features in 4.2(2a)

New Software Features in Release 4.2(2a)

The following new software features are supported in Release 4.2(2a):

- Support for UCSC-9400-8E - Cisco 9400-8e 12G SAS HBA in Cisco UCS S3260 M5 servers.
- Beginning with release 4.2(2a), Cisco IMC supports priority tagging or Physical NIC mode on the Cisco UCS M5, S3260 M5 and M6 servers equipped with Cisco UCS VIC 14xx or UCS VIC 15xxx series cards.

  This option is disabled by default. When Physical NIC Mode is enabled, up-link ports of the VIC are set to pass-through mode. This allows the host to transmit packets without any modification. VIC ASIC does not rewrite the VLAN tag of the packets based on the VLAN and CoS settings for the vNIC.

Note

- This option cannot be enabled on an adapter that has:
    - **Port Channel mode** enabled
    - **VNTAG mode** enabled
    - **LLDP** enabled
    - **FIP mode** enabled
    - **Cisco IMC Management Enabled** value set to **Yes**

  Ensure that the above options are disabled before you enable **Physical NIC Mode**.
- Only the default 2 or 4 vNICs should be used (depending on the type of adapter).
- iSCSI or other storage network technologies are not supported.
- The following are not supported with **Physical NIC Mode**:
    - usNIC
    - Geneve offload
    - Cisco card mode
- When you disable **Physical NIC Mode** from Cisco IMC, you must manually enable all the other required features. Select **Reset to Defaults** to reset the vNIC configuration on the adapter to its default settings.

For more details, see Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide, Release 4.2 or Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Release 4.2.

- Beginning with release 4.2(2a), Cisco IMC supports disabling TLS v1.2 and also customizing the cipher values for both v1.2 and v1.3.
- Beginning with 4.2(2a) release, Cisco IMC allows you to upload up to ten certificates for configured secure HTTP Boot device. You can also delete and upload a new certificate for the specific boot device configured. Cisco IMC allows you to upload up to ten root CA Certificates.
- Secure Syslog on Standalone and FI-attached servers —Beginning with release 4.2(2a), Cisco IMC allows users to establish a secure, encrypted outbound connection to remote syslog servers (acting as a server), supporting secure connectivity for logging.

  For more details, see Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide, Release 4.2 or Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Release 4.2.
- Drive Diagnostics feature on SAS/SATA drive types —Beginning with release 4.2(2a), you can perform drive diagnostic self-test on SATA drives also. For more details, see Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Release 4.2.

Note This feature does not support NVME JBOD drives. You may use third-party tools to diagnose NVME JBOD disk errors.

- Beginning with 4.2(2a) release, Cisco IMC supports a new HUU user interface. For more details, see Cisco Host Upgrade Utility User Guide, Release 4.2.
- Support to enable **PCIe Slots CDN Control** option.
- Support for Redfish API support for eMMC functionality.
- Support for Redfish API for Cisco UCS S3260 M4 and M5 servers.
- Clearing Personality Configuration —Beginning with release 4.2(2a), you can clear the personality configuration by using the command-line interface.

  For more details, see Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Release 4.2.
- **Enable Video Encryption** check box option has been deprecated.
- Support for reading PCIe connected device data including firmware version.

New Hardware Features in Release 4.2

New Hardware in Release 4.2(2f)

Support for the following:

- Nvidia GPU-A100-80 GPU (UCSC-GPU-A100-80) for Cisco UCS M5 and M6 servers.
- Nvidia GPU-A30 GPU (UCSC-GPU-A30) for Cisco UCS C245 M6 and C240 M6 servers.

New Hardware in Release 4.2(2a)

Peripherals

Support for the following:

- UCS-M2-HWRAID - Cisco M.2 Boot Optimized RAID Controller on Cisco UCS M6 servers now supports both single and dual drive configurations.
- Support for UCS VIC 15428 on Cisco UCS M6 servers.

  SFP-10G-T-X transceiver is supported with VIC 15428 on the ports 2 and 4, when in standby-power. When the server is fully powered-on, SFP-10G-T-X transceiver is enabled for all the 4 ports. If you mix cable types on a 15428 VIC card along with SFP-10G-T-X, the ports 1 and 3 support only passive copper cables (10/25G).
- Intel X710T4LG 4x10 GbE RJ45 PCIe NIC (Carlsville ASIC) with Cisco UCS C220 M6, C240 M6, C225 M6, and C245 M6 servers.
- Qlogic QLE 2772 Fibre Channel Adapter with Cisco UCS C125 M5 servers.
- Qlogic QLE 2772 or QLE 2742 Fibre Channel Adapter with Cisco UCS S3260 servers.

- QLogic QLE2772 2x32GFC Gen 6 Enhanced PCIe HBA) with Cisco UCS C225 M6 and C245 M6 servers
- MLNX MCX623106AS-CDAT, 2x100 GbE QSFP56 PCIe (non-Crypto/TLS) with Cisco UCS C225 M6 and C245 M6 servers.
- UCSC-P-B7D32GF (Cisco-Emulex LPe35002-M2-2x32GFC Gen 7 PCIe HBA)

Security Fixes

Security Fixes in Release 4.2(2f)

The following Security Fixes were added in Release 4.2(2f):

Defect ID - CSCwb67205

Cisco UCS C-Series M6 Rack Servers include an Intel CPU that is affected the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID(s):

- **CVE-2022-0005**—Sensitive information accessible by physical probing of JTAG interface for some Intel® Processors with SGX may allow an unprivileged user to potentially enable information disclosure through physical 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.
- **CVE-2022-21151**—Processor optimization removal or modification of security-critical code for some Intel® Processors may allow an authenticated user to potentially enable information disclosure through local access.
- **CVE-2021-33060**—Users have access to the directory where the installation repair occurs. Since the MS Installer allows regular users to run the repair, an attacker can initiate the installation repair and place a specially crafted EXE in the repair folder which runs with the Check Point Remote Access Client privileges.
- **CVE-2022-21233**—Stale data may be returned as the result of unauthorized reads to the legacy xAPIC MMIO region. This issue is present only in the legacy xAPIC mode and does not affect the x2APIC mode. This can be used to expose sensitive information in an SGX enclave.

Security Fixes in Release 4.2(2a)

The following Security Fixes were added in Release 4.2(2a):

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 - CSCvw39931

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

- **CVE-2020-8690**—Protection mechanism failure in Intel(R) Ethernet 700 Series Controllers before version 7.3 may allow a privileged user to potentially enable escalation of privilege or denial of service via local access.
- **CVE-2020-8691**—A logic issue in the firmware of the Intel(R) Ethernet 700 Series Controllers may allow a privileged user to potentially enable escalation of privilege or denial of service via local access.
- **CVE-2020-8691**—Insufficient access control in the firmware of the Intel(R) Ethernet 700 Series Controllers before version 7.3 may allow a privileged user to potentially enable escalation of privilege or denial of service via local access.
- **CVE-2020-8691**—Improper buffer restrictions in the firmware of the Intel(R) Ethernet 700 Series Controllers may allow a privileged user to potentially enable escalation of privilege or denial of service via local access.

Defect ID - CSCvy53109

Cisco UCS C220 M5 server is affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- **CVE-2019-20006**—An issue was discovered in ezXML 0.8.3 through 0.8.6. The function ezxml_char_content puts a pointer to the internal address of a larger block as xml->txt. This is later deallocated (using free), leading to a segmentation fault.
- **CVE-2021-26220**—The ezxml_toxml function in ezxml 0.8.6 and earlier is vulnerable to OOB write when opening XML file after exhausting the memory pool.
- **CVE-2021-26221**—The ezxml_new function in ezXML 0.8.6 and earlier is vulnerable to OOB write when opening XML file after exhausting the memory pool.
- **CVE-2021-26222**—The ezxml_new function in ezXML 0.8.6 and earlier is vulnerable to OOB write when opening XML file after exhausting the memory pool.
- **CVE-2021-31598**—An issue was discovered in libezxml.a in ezXML 0.8.6. The function ezxml_decode() performs incorrect memory handling while parsing crafted XML files, leading to a heap-based buffer overflow.

Defect ID - CSCvz49944

After power cycle, Cisco UCS C125 M5 server is unable to boot from the SD card as Hypervisor is not reachable.

Defect ID - CSCvz49660

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

- **CVE-2021-3711**—In order to decrypt SM2 encrypted data, an application is expected to call the API function `EVP_PKEY_decrypt()`. An application calls this function twice. During the first time, on entry, the "out" parameter can be NULL and, on exit, the "outlen" parameter is populated with the buffer size required to hold the decrypted plaintext. The application can then allocate a sufficiently sized buffer and call `EVP_PKEY_decrypt()` again. However, this time, it passes a non-NULL value for the "out" parameter.

  A bug in the implementation of the SM2 decryption code means that the calculation of the buffer size required to hold the plain text returned by the first call to `EVP_PKEY_decrypt()` can be smaller than the actual size required by the second call. This can lead to a buffer overflow when `EVP_PKEY_decrypt()` is called by the application a second time with a buffer that is too small.

  An attacker who can present SM2 content for decryption to an application could cause attacker-chosen data to overflow the buffer by upto a maximum of 62 bytes, altering the contents of other data held after the buffer. This can also change application behaviour or cause the application to crash. The location of the buffer is application-dependent but is heap-allocated. Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k).

Defect ID - CSCvz83417

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

- **CVE-2019-20005**—An issue was discovered in ezXML 0.8.3 through 0.8.6. While parsing a crafted XML file, the function ezxml_decode performs incorrect memory handling, leading to a heap-based buffer over-read while running `strchr()` starting with a pointer after a '\0' character (where the processing of a string was finished).

- **CVE-2019-20006**—An issue was discovered in ezXML 0.8.3 through 0.8.6. The function `ezxml_char_content` puts a pointer to the internal address of a larger block as xml to txt. This is later de-allocated (using free), leading to a segmentation fault.

- **CVE-2019-20007**—An issue was discovered in ezXML 0.8.2 through 0.8.6. While parsing a crafted XML file, the function `ezxml_str2utf8` performs zero-length re-allocation in `ezxml.c`, leading to returning a NULL pointer (in some compilers). After this, the function `ezxml_parse_str` does not check whether the `s` variable is not NULL in `ezxml.c`, leading to a NULL pointer dereference and crash (segmentation fault).

- **CVE-2019-20198**—An issue was discovered in ezXML 0.8.3 through 0.8.6. The function `ezxml_ent_ok()` mishandles recursion, leading to stack consumption for a crafted XML file.

- **CVE-2019-20199**—An issue was discovered in ezXML 0.8.3 through 0.8.6. While parsing a crafted XML file, the function `ezxml_decode`, performs incorrect memory handling, leading to NULL pointer dereference while running `strlen()` on a NULL pointer.

- **CVE-2019-20200**—An issue was discovered in ezXML 0.8.3 through 0.8.6. While parsing crafted a XML file, the function `ezxml_decode`, performs incorrect memory handling, leading to a heap-based buffer over-read in the **normalize line endings** feature.

- **CVE-2019-20201**—An issue was discovered in ezXML 0.8.3 through 0.8.6. The `ezxml_parse_*` functions mishandle XML entities, leading to an infinite loop in which memory allocations occur.

- **CVE-2019-20202**—An issue was discovered in ezXML 0.8.3 through 0.8.6. The function `ezxml_char_content()` uses realloc on a block that was not allocated, leading to an invalid free and segmentation fault.
- **CVE-2021-26220**—The `ezxml_toxml` function in ezxml 0.8.6 and earlier is vulnerable to OOB write while opening XML file, after exhausting the memory pool.
- **CVE-2021-26221**—The `ezxml_new` function in ezXML 0.8.6 and earlier is vulnerable to OOB write while opening XML file, after exhausting the memory pool.
- **CVE-2021-26222**—The `ezxml_new` function in ezXML 0.8.6 and earlier is vulnerable to OOB write while opening XML file, after exhausting the memory pool.
- **CVE-2021-30485**—An issue was discovered in libezxml.a in ezXML 0.8.6. While parsing a crafted XML file, the function `ezxml_internal_dtd()` performs incorrect memory handling, leading to a NULL pointer dereference while running `strcmp()` on a NULL pointer.
- **CVE-2021-31229**—An issue was discovered in libezxml.a in ezXML 0.8.6. While parsing crafted XML files, the function `ezxml_internal_dtd()` performs incorrect memory handling, leading to an out-of-bounds write of a one byte constant.
- **CVE-2021-31347**—An issue was discovered in libezxml.a in ezXML 0.8.6. The function `ezxml_parse_str()` performs incorrect memory handling while parsing crafted XML files (writing outside a memory region created by mmap).
- **CVE-2021-31348**—An issue was discovered in `libezxml.a` in ezXML 0.8.6. While parsing crafted XML files, the function `ezxml_parse_str()` performs incorrect memory handling (out-of-bounds read after a certain strcspn failure).
- **CVE-2021-31598**—An issue was discovered in `libezxml.a` in ezXML 0.8.6. While parsing crafted XML files, the function `ezxml_decode()` performs incorrect memory handling, leading to a heap-based buffer overflow.

Defect ID - CSCwb67158

Cisco UCS M4 servers (excluding Cisco UCS C460 M4) are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- **CVE-2021-0153**—Out-of-bounds write in the BIOS firmware for some Intel$^{(R)}$ Processors might allow a privileged user to enable escalation of privilege through local access.
- **CVE-2021-0154**—Improper input validation in the BIOS firmware for some Intel$^{(R)}$ Processors might allow a privileged user to enable aescalation of privilege through local access.
- **CVE-2021-0155**—Unchecked return value in the BIOS firmware for some Intel$^{(R)}$ Processors might allow a privileged user to enable information disclosure through local access.
- **CVE-2021-0190**—Uncaught exception in the BIOS firmware for some Intel$^{(R)}$ 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$^{(R)}$ 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$^{(R)}$ Processors might allow a privileged user to enable escalation of privilege through local access.

Defect ID - CSCwb67157

Cisco UCS C460 M4 servers 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(R) Processors might allow a privileged user to enable aescalation of privilege through local access.
- **CVE-2021-0155**—Unchecked return value in the BIOS firmware for some Intel(R) Processors might allow a privileged user to enable information disclosure through local access.
- **CVE-2021-0189**—Uncaught exception in the BIOS firmware for some Intel(R) 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(R) 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(R) Processors might allow a privileged user to enable escalation of privilege through local access.

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.

Resolved Caveats

Resolved Caveats in 4.2(2g)

The following defects were resolved in Release 4.2(2g):

Table 21: BIOS

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwd18446	Cisco UCS HX240-M6 server equipped with HX-PCIE-OFFLOAD-1 and UCS 4.2(1n) fails at deploy stage of the installer with various GUI errors. This issue is now resolved.	4.2(1j)	4.2(2g)

Table 22: BMC Storage

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwd03250	In Cisco UCS servers with Cisco UCS 4.2(2a) firmware and equipped with drives configured as Global Hot Spare/Unconfigured Good and drive self test feature enabled, the following fault might be displayed: Local disk X is degraded. This issue is now resolved.	4.2(2a)	4.2(2g)

Resolved Caveats in 4.2(2f)

The following defects were resolved in Release 4.2(2f):

Table 23: CMC

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvz47731	If the timezone is directly changed on Cisco IMC servers and is not supported in Intersight, then the default timezone will be shown in **Configuration Drift** in the server profile detail view in Intersight. This issue is now resolved.	4.2(2f)	4.2(2f)

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwb46682	In Cisco UCS S3260 M5 servers equipped with PCI SIOC with UCS VIC 1455 in 1st SIOC and QLE2692 in 2nd SIOC (single server with dual SIOC configured in Single IP mode), when active CMC is rebooted, Cisco IMC does not fail over to the stand-by SIOC. This issue is now resolved.	4.2(2f)	4.2(2f)

Table 24: BMC

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwc46398	In Cisco UCS servers equipped with VIC 14xx and enabled with multi-queue configuration, Cisco IMC UI shows incorrect values for Receive / Transmit / Completion Queue Count parameters. This issue is now resolved.	4.1(3f)	4.2(2f)
CSCwc06871	Cisco UCS M5 server configured with default settings and with Cisco IMC allows SSH connections. This can be leveraged by a malicious user. This issue is now resolved.	4.1(3f)	4.2(2f)

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwc47846	The value of the **Class of Service** field in the **RoCE Properties** section is not updated in Cisco IMC UI. This occurs in Cisco UCS M5 servers equipped with VIC card configured with RDMA and multi-queue using Intersight server profile and policy. This issue is now resolved.	4.1(3f)	4.2(2f)

Table 25: SNMP

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvz61901	When the DIMM is reported as failed in Cisco IMC, the object identifier reports the status as **unknown**. This issue is now resolved.	4.1(1c)	4.2(2f)

Table 26: External LSI SAS Controller

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwc18223	In Cisco UCS C240 M6 servers, one or more SED drives are marked as **unconfigured good** after server reboot. This issue is now resolved.	4.2(1f)	4.2(2f)

Open Caveats

The following section lists open caveats.

Open Caveats in 4.2(2f)

The following defect is open in Release 4.2(2f):

Table 27: BMC Storage

Defect ID	Symptom	Workaround	First Affected Release
CSCwc70846	Cisco UCS servers equipped Solidigm ADP RR drives shows incorrect drive size, protocol and drive type in IMM UI.	There are no known workarounds. You may find the NVMe SSD size from the **Model** field or UCS PID. The drive protocol and type is implicit.	4.2(2f)

Open Caveats in 4.2(2a)

The following defects are open in Release 4.2(2a):

Table 28: Hardware

Defect ID	Symptom	Workaround	First Affected Release
CSCwb92046	Under certain high cluster utilization conditions, the drive displays I/O failures in Cisco UCS C240 M6 servers. The drive failure details are not captured in the drive diagnostic report.	Reboot the host and perform the drive diagnostics.	4.2(2a)

Table 29: BIOS

Defect ID	Symptom	Workaround	First Affected Release
CSCvz28553	Cisco UCS C245 M6 servers equipped with Cisco UCS VIC 1495 in slot 4 and running RHEL OS, **Consistent Device Naming** (CDN) name from Cisco IMC does not get correctly reported and appears differently in the OS.	You may use Cisco UCS VIC 1455 card Riser 1, slot 1.	4.2(1c)

Defect ID	Symptom	Workaround	First Affected Release
CSCwa26477	When you open the Cisco IMC Configuration Utility with VLAN enabled, a warning message is displayed in the first attempt while switching from standalone to Cisco Card mode. This issue occurs due to the mismatch in the selection of VLAN settings.	Perform the following steps: 1. During the boot up, enter the **F8** (Cisco IMC Configuration Utility). 2. Press **F10** to save the updated settings. The warning message is not displayed.	4.2(2a)

Table 30: BMC

Defect ID	Symptom	Workaround	First Affected Release
CSCwb41346	In a setup equipped with Cisco UCS M5 servers and Cisco VIC 1385 cards, FcIfs creation XML query displays invalid PCI order error (0,1) for PCI order 2, and (0,2) for PCI order 3. This issue occurs only when you configure the PCI link as **0** for second default vNIC present for the Cisco VIC 1385.	Do not send PCI Link for the second adapter in the request. All other parameters given in the request for modification, will be modified successfully.	4.1(2f)
CSCwb45042	In a setup equipped with Cisco UCS M6 server and Cisco VIC 15xxx card in MLOM slot, an error log event in Cisco IMC SEL is recorded with the following message: `MLOM_FAN_SPEED: Fan sensor, non-recoverable event, Lower Non-Recoverable going low (0 <= 0 RPM) was asserted.`	You can ignore this Cisco IMC SEL error log event. This fault does not have any impact on the functionality.	4.2(2a)

Known Behaviors and Limitations

Known Behaviors and Limitations in Release 4.2(2a)

The following caveats are known limitations in release 4.2(2a):

Table 31: BMC Storage

Defect ID	Symptom	Workaround	First Affected Release
CSCwc64817	In Cisco UCS S3260 M5 servers running Cisco IMC release 4.2(2a): 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)

Table 32: BMC

Defect ID	Symptom	Workaround	First Affected Release
CSCvy89810	In Cisco UCS C245 M6 servers, if **NIC Mode** is configured as **Shared OCP Extended**, then BMC becomes inaccessible after downgrading to release 4.2(1a).	Perform the following steps to recover the Cisco IMC network: **1.** Connect the local monitor to VGA port. **2.** Reboot the host using the power button. **3.** During the boot up, enter the **F8** (Cisco IMC Configuration Utility) and choose **Factory Defaults** option. **4.** Press **F10** to save. Cisco IMC reboots to factory default settings. If VIC is populated in the supported riser slots, **NIC Mode** switches to **Cisco Card** mode. If there is no VIC, **NIC mode**switches to **Dedicated** mode. Reboot the host again and enter the **F8** utility to configure the network settings.	4.2(1c)
CSCvz75479	Mounting and uploading files using the SMB 1.0 protocol fails in all Cisco IMC interfaces.	Manually add `vers=1.0` mount option while uploading or mounting the files using the SMB 1.0 protocol.	4.2(2a)

Defect ID	Symptom	Workaround	First Affected Release
CSCwb01860	In Cisco UCS M6 servers, storage firmware downgrade fails with the following message: `Failed: flash image not supported` This issue occurs in Cisco UCS M6 servers equipped with the following: • Adaptors with PCIe vendor id 1000h and device id 10E2h • Firmware: MR 7.20 and above in the system and downgraded to 7.19 or below	Upgrade to the latest patch that contains the storage firmware version 7.20.	4.2(2a)
CSCwb71501	In Cisco UCS M6 server BIOS settings, the default value for **memory refresh rate** is 2x refresh rate. However, the BIOS changes the value of **memory refresh rate** to 1x refresh rate for 128 and 256 DIMMs.	No known workaround.	4.2(2a)

Limitation

Issue

In a setup equipped with Cisco UCS C225 M6 or C245 M6 server and Cisco VIC 15xxx card in MLOM slot and connected with 25G cable, Cisco IMC becomes inaccessible when the following option is configured with the default value:

- **Admin FEC Mode** is set to **c191**.

Workaround

Perform the following steps to set **Admin FEC Mode** to the appropriate value and access Cisco IMC:

1. Reboot the host using the power button.
2. During the boot up, enter the **F8** (Cisco IMC Configuration Utility).

   Set the **NIC mode** to **Dedicated** mode

3. Reboot the host and log in to Cisco IMC.
4. In the **Navigation** pane, click the **Networking** menu.
5. In the **Networking** menu, select the adapter card that you want to view.
6. Click the **External Ethernet Interfaces** link.

   External Ethernet Interfaces opens in a different tab.
7. Set the **Admin FEC Mode** to **c174**.

Note This issue does not occur when Cisco UCS C225 M6 or C245 M6 server contains Cisco VIC 15xxx card in MLOM slot and connected with 10G cable.

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:

- 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