Release Notes for Cisco UCS Rack Server Software, Release 4.3(2)

First Published: 2023-08-16

Last Modified: 2024-03-05

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 4.3(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 35 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
D0	March 05, 2024	Created release notes for 4.3.2.240009 for the following servers: • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers • Cisco UCS C220 M5, C240 M5, C480 M5, C125 M5 and S3260 M5 servers
A1	February 22, 2024	Updated the **Open Caveats** section for the release 4.3.2.230207
C1	February 02, 2024	Updated the **Security Fixes** section for the release 4.3.2.240002

Revision	Date	Description
C0	January 23, 2024	Created release notes for 4.3.2.240002 for the following servers: • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers • Cisco UCS C220 M5, C240 M5, C480 M5, C125 M5 and S3260 M5 servers
B0	November 14, 2023	Created release notes for 4.3.2.230270 for the following servers: • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers • Cisco UCS C220 M5, C240 M5, C480 M5, C125 M5 and S3260 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 4.3

Revision	Date	Description
A0	August 16, 2023	Created release notes for 4.3.2.230207 for the following servers: • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers • Cisco UCS C220 M5, C240 M5, C480 M5, C125 M5 and S3260 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 4.3

Cisco IMC Release Number and .ISO Image Names

Beginning with the release 4.3, Cisco is updating the release number naming convention to align with the .ISO images.

Example: **4.3.1.YYXXXX**

- **4.3**—Represents the main release.
- **.1**—Represents the first release.

  For the current 4.3 main release, **.1** represents the first release number.

  For subsequent maintenance releases, this number will represent the related maintenance release number.
- **YY**—Represents the year of release.

  For the current 4.3 main release, **23** is derived from the year 2023.
- **XXXX**—The final 4 digits represent the increasing sequence of build numbers every year.

  For the first 4.3 main release, the number is **0097**.

Supported Platforms and Release Compatibility Matrix

Supported Platforms in this Release

The following servers are supported in this release:

- Cisco UCS C220 M7
- Cisco UCS C240 M7

- 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 C480 ML M5
- Cisco UCS C125 M5
- Cisco UCS S3260 M5

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 4.3(2) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.3.2.240009	NA	• Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers • Cisco UCS C220 M5, C240 M5, C480 M5, C125 M5 and S3260 M5 servers
4.3.2.240002	4.3(2)	• Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers • Cisco UCS C220 M5, C240 M5, C480 M5, C125 M5 and S3260 M5 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.3.2.230270	4.3(2)	• Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers • Cisco UCS C220 M5, C240 M5, C480 M5, C125 M5 and S3260 M5 servers
4.3.2.230207	4.3(2)	• Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers • Cisco UCS C220 M5, C240 M5, C480 M5, C125 M5 and S3260 M5 servers

Table 2: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.3(1) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.3.1.230138	No Support	Cisco UCS C220 M7 and C240 M7 servers
4.3.1.230124	No Support	Cisco UCS C220 M7 and C240 M7 servers
4.3.1.230097	No Support	Cisco UCS C220 M7 and C240 M7 servers

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

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.2(3j)	4.2(3j)	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

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.2(3i)	4.2(3i)	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(3g)	4.2(3g)	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(3e)	4.2(3e)	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(3d)	4.2(3d)	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(3b)	4.2(3b)	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 4: 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

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount 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 5: 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 6: 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

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount 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
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 7: 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

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount 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
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 8: 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

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount 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

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 4.3(2):

Recommended Browser	Minimum Recommended Browser Version	Minimum Recommended Operating System
Google Chrome	Version 114.0.5735.198 (Official Build) (x86_64)	Mac OS 13.4.1 (22F82)
	Version 112.0.5615.138 (Official Build) (64-bit)	Microsoft Windows 2019
	Version 114.0.5735.199 (Official Build) (64-bit)	Microsoft Windows Server 2019
	Version 115.0.5790.110 (Official Build) (64-bit)	Microsoft Windows 11 Enterprise
	Version 109.0.5414.149 (Official Build) (64-bit)	Microsoft Windows 2019
	Version 115.0.5790.110 (Official Build) (64-bit)	Microsoft Windows 11 Enterprise
Safari	Version 16.6 (18615.3.12.11.2)	Mac OS 13.5 (22G74)
	Version 16.5.2 (18615.2.9.11.10)	Mac OS 13.4.1 (22F82)
Mozilla Firefox	115.0.3 (64-bit)	Mac OS 13.5 (22G74)
	116.0 (64-bit)	Microsoft Windows 11 Enterprise

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.

Default Ports

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

Table 9: 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
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 and Downgrade Guidelines

To get a complete overview of all the possible upgrade paths in Cisco IMC, see Cisco UCS Rack Server Upgrade Support Matrix.

Infrastructure Upgrade and Downgrade to Release 4.3(2):

- Cisco UCS M4 servers are not supported by 4.3.2.230207 and later releases.
- You must perform firmware update after adding any new hardware component to the system.
- If you are planning to install Cisco UCS VIC 15237 or 15427 in a server, then upgrade the server to 4.3.2.230270 or later versions and then insert the adapter into the server.

If you insert Cisco UCS VIC 15237 or 15427 into the server that is running earlier versions than 4.3.2.230270, then upgrade the server to 4.3.2.230270 or later versions and power cycle the server to recognize the adapter.

- If you are planning to install Cisco UCS VIC 15235 or 15425 in a server, then upgrade the server to 4.3.2.230207 or later versions and then insert the adapter into the server.

  If you insert Cisco UCS VIC 15235 or 15425 into the server that is running earlier versions than 4.3.2.230207, then upgrade the server to 4.3.2.230207 or later versions and power cycle the server to recognize the adapter.

Support for Cisco UCS M7 Servers

Cisco UCS M7 servers are supported from the release 4.3.1.230097 onwards.

The following releases are for Cisco UCS M7 servers only:

- 4.3.1.230138
- 4.3.1.230124
- 4.3.1.230097

Upgrade Paths to Release 4.3.2

The section provides information on the upgrade paths to release 4.3.2.

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

Table 10: Upgrade Paths to Release 4.3(2x)

Upgrade From Release	Upgrade To Release	Recommended Upgrade Path
Following Cisco UCS servers from the release 4.3.1.230097 • Cisco UCS C220 M7 • Cisco UCS C240 M7	• 4.3.2.240002 • 4.3.2.230270 • 4.3.2.230207 • 4.3.1.230138 • 4.3.1.230124	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 4.3.2.230207. • 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 the release 4.2(3b) • 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 C480 M5 ML • Cisco UCS S3260 M5 • Cisco UCS C125 M5	• 4.3.2.240009 • 4.3.2.240002 • 4.3.2.230270 • 4.3.2.230207 • 4.2(3g) • 4.2(3e) • 4.2(3d)	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 4.3.2.230207. • 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 the release 4.2(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	• 4.3.2.240009 • 4.3.2.240002 • 4.3.2.230270 • 4.3.2.230207 • 4.2(3g) • 4.2(3e) • 4.2(3d) • 4.2(3b)	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 4.2.2. • 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.

Upgrade From Release	Upgrade To Release	Recommended Upgrade Path
All Cisco UCS M6 Servers from 4.2(1). For the list of supported platforms, see Table 11: Upgrade Paths to Release 4.2(1a), on page 16.	• 4.3.2.240009 • 4.3.2.240002 • 4.3.2.230270 • 4.3.2.230207	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(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 4.1(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	• 4.3.2.240009 • 4.3.2.240002 • 4.3.2.230270 • 4.3.2.230207 • 4.2(3g) • 4.2(3e) • 4.2(3d) • 4.2(3b)	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	• 4.3.2.240009 • 4.3.2.240002 • 4.3.2.230270 • 4.3.2.230207 • 4.2(3g) • 4.2(3e) • 4.2(3d) • 4.2(3b)	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	• 4.3.2.240009 • 4.3.2.240002 • 4.3.2.230270 • 4.3.2.230207 • 4.2(3g) • 4.2(3e) • 4.2(3d) • 4.2(3b)	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	• 4.3.2.240009 • 4.3.2.240002 • 4.3.2.230270 • 4.3.2.230207 • 4.2(3g) • 4.2(3e) • 4.2(3d) • 4.2(3b)	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.

Table 11: Upgrade Paths to Release 4.2(1a)

Upgrade From Release	Upgrade To Release	Recommended Upgrade Path
Cisco UCS C220 M6 Cisco UCS C240 M6 Cisco UCS C225 M6 Cisco UCS C245 M6	• 4.3.2.240002 • 4.3.2.230270 • 4.3.2.230207 • 4.2(3g) • 4.2(3e) • 4.2(3d) • 4.2(3b)	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(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.

Firmware Files

Firmware Files

The C-Series software release 4.3.2.230207 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 4.3	Host Upgrade Utility
Unified Computing System (UCS) Drivers	ucs-cxxx-drivers.4.3.2.230207.iso	Drivers
Unified Computing System (UCS) Utilities	ucs-cxxx-utils-efi.4.3.2.230207.iso ucs-cxxx-utils-linux.4.3.2.230207.iso ucs-cxxx-utils-vmware.4.3.2.230207.iso ucs-cxxx-utils-windows.4.3.2.230207.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 4.3.

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
- Broadcom Adapters
- LAN on Motherboard
- PCIe adapter firmware
- HDD firmware
- SAS Expander firmware
- DCPMM Memory
- PCI Gen5 retimer

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

SNMP

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

https://cisco.github.io/cisco-mibs/

Software Utilities

The following standard utilities are available:

- Host Update Utility (HUU)
- 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.

New Hardware in Release 4.3.2

New Hardware in Release 4.3.2.230270

Cisco UCS VIC Cards

Following Cisco UCS secure boot enabled VIC cards are supported from the release 4.3.2.230270 onwards:

- Cisco UCS VIC 15427 (UCSC-M-V5Q50GV2) — The Cisco UCS VIC 15427 is a quad-port small-form-factor pluggable (SFP+/SFP28/SFP56) mLOM card designed for Cisco UCS C-series M6/M7 rack servers. The card supports 10/25/50-Gbps Ethernet or FCoE. The card can present PCIe standards-compliant interfaces to the host, and these can be dynamically configured as either NICs or HBAs.
- Cisco UCS VIC 15237 (UCSC-M-V5D200GV2) — The Cisco UCS VIC 15237 is a dual-port small-form-factor pluggable (QSFP/QSFP28/QSFP56) mLOM card designed for Cisco UCS C-series M6/M7 rack servers. The card supports 40/100/200-Gbps Ethernet or FCoE. The card can present PCIe standards-compliant interfaces to the host, and these can be dynamically configured as either NICs or HBAs.

Note

- If you are planing to install Cisco UCS VIC 15427 or 15237, then ensure that you first upgrade the servers to release 4.3.2.230270, and then install the adapters in the server. If you install the adapters into the server running an earlier release, and then upgrade the servers to release 4.3.2.230270, the servers require A/C power cycle to recognize the adapters.
- Cisco UCS VIC 15427 or VIC 15237 does not support VIC 14xx PCIe cards on Cisco UCS M6 servers.
- Cisco UCS C-series M7 servers do not support VIC 1400 series adapters

New Hardware in Release 4.3.2.230207

Cisco UCS VIC Cards

Following Cisco UCS secure boot enabled VIC cards are supported from the release 4.3.2.230207 onwards:

- Cisco UCS VIC 15425 (UCSC-P-V5Q50G)—The Cisco UCS VIC 15425 is a quad-port small-form-factor pluggable (SFP+/SFP28/SFP56) PCIe card designed for Cisco UCS C-series M6/M7 rack servers. The card supports 10/25/50-Gbps Ethernet or FCoE. The card can present PCIe standards-compliant interfaces to the host, and these can be dynamically configured as either NICs or HBAs.
- Cisco UCS VIC 15235 (UCSC-P-V5D200G)—The Cisco UCS VIC 15235 is a dual-port quad small-form-factor pluggable (QSFP/QSFP28/QSFP56) PCIe card designed for Cisco UCS C-series M6/M7 rack servers. The card supports 40/100/200-Gbps Ethernet or FCoE. The card can present PCIe standards-compliant interfaces to the host, and these can be dynamically configured as either NICs or HBAs.

Note

- If you are planing to install Cisco UCS VIC 15235 or 15425, then ensure that you first upgrade the servers to release 4.3(2) and then install the adapters in the server. If you install the adapters into the server running an earlier release, and then upgrade the servers to release 4.3(2), the servers require A/C power cycle to recognize the adapters.
- Cisco UCS C-series M7 servers do not support VIC 1400 series adapters

Peripherals

Following peripherals are supported from the release 4.3.2.230207 onwards:

- Cisco boot optimized M.2 NVMe RAID controller (UCS-M2-NVRAID) - Supported on Cisco UCS C220 M7 and C240 M7 servers
- Cisco-QLogic QLE2872, 2x64GFC Gen 7 PCIe HBA (UCSC-P-Q7D64GF) - Supported on Cisco UCS C-Series M6 and M7 servers
- Cisco-NVDA MCX623436AC-CDAB CX6Dx 2x100G QSFP56 x16 OCP NIC (UCSC-O-N6CD100GF) - Supported on Cisco UCS C220 M6 and UCS C240 M6 servers
- Cisco-NVDA MCX631432AC-ADAB CX6 Lx 2x25G SFP28 x8 OCP NIC (UCSC-O-N6CD25GF) - Supported on Cisco UCS C220 M6 and C240 M6 servers
- Cisco Tri-Mode 24G SAS RAID Controller w/4GB Cache (UCSC-RAID-HP) - Supported on Cisco UCS C220 M7 and C240 M7 servers

Supported GPUs

The following are the list of new GPUs supported from the release 4.3.2.230207 onwards:

- Intel Data Center GPU Flex 140, HHHL, 75W PCIe (UCSC-GPU-FLEX140) - Supported on Cisco UCS C220 M7 and UCS C240 M7 servers
- Intel Data Center GPU Flex 170, FH-3/4L 150W, PCIe (UCSC-GPU-FLEX170) - Supported on Cisco UCS C240 M7 servers.
- Nvidia H100 350W, 80GB, 2-slot FHFL PCIe GPU (UCSC-GPU-H100-80) - Supported on Cisco UCS C240 M7 servers
- Nvidia L40, 300W, 48GB, 2-slot FHFL PCIe GPU (UCSC-GPU-L40) - Supported on Cisco UCS C240 M7 servers

- Nvidia L4, 72W, 24GB, single-slot HHHL PCIe GPU (UCSC-GPU-L4) - Supported on Cisco UCS C220 M7 servers

New Software in Release 4.3.2

New Software Features in Release 4.3.2.230207

The following new software features are supported in Release 4.3.2.230207.

- Support for Q-in-Q tunneling configuration: A Q-in-Q (802.1Q-in-802.1Q) tunnel allows to segregate the traffic in the infrastructure and helps to expand the VLAN space through the addition of 802.1Q tag to 802.1Q-tagged packets.
- Support for Secure Boot on Cisco UCS VIC 15235 and 15425 Virtual Interface Cards (VIC) on Cisco UCS C-Series servers.

  Secure Boot is a trustworthy technology that ensures the code running on Cisco hardware platforms is authentic, unmodified, and operational as intended. The Secure Boot uses a trust anchor module (TAm) in hardware to verify the bootloader code. It also protects the boot code in hardware and checks digitally signed images to verify that only genuine, unmodified code boots on a Cisco device.
- Added Windows NENIC Driver support to enable Receive Side Scaling Version 2 (RSSv2) for Cisco UCS VIC 15000 series adapters.

  Receive Side Scaling (RSS) supports multiple cores to process the incoming data traffic. When RSS is enabled on the VIC, multiple hardware receive queues can be configured on the Physical Function (PF). In general, a NENIC driver supports 4 queues. With RSSv2, the NENIC driver has no upper limit on the number of hardware queues for PF or VM.

  RSSv2 is supported on Cisco UCS C-Series M6 and M7 servers.
- Support of SRIOV on Cisco UCS VIC 1400 series adapters.

Resolved Caveats

Resolved Caveats in Release 4.3.2.240009

The following defects were resolved in Release 4.3.2.240009:

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwj00617	In Cisco UCS M5 and M6 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)	4.3.2.240009

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwi97945	In Cisco UCS M5 and M6 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)	4.3.2.240009

Resolved Caveats in Release 4.3.2.240002

The following defects were resolved in Release 4.3.2.240002:

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwh45111	In Cisco IMC, connectivity is lost when the host is powered off and the system network configuration is set to Cisco card mode and M.2 controller card present in the system. This issue is now resolved.	4.2(3d)	4.3.2.240002
CSCwh53073	The date and time is shown incorrectly as **in 9 hours** in the **Alarm** page in the Intersight UI. The values for the alarms are generated from Cisco IMC. This issue is now resolved.	4.3.2.230207	4.3.2.240002

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwi04192	in Cisco UCS C220 M6 and C240 M6 servers with UCSC-O-N6CD100GF Mellanox card, the third party MLOM cards overheat and flap links as the default fan policy are not sufficient to cool down the card. This issue is now resolved.	4.3.2.230207	4.3.2.240002

Resolved Caveats in Release 4.3.2.230270

The following defects were resolved in Release 4.3.2.230270:

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwf71163	Configuring SRIOV on non default interfaces and rebooting the host might affect the existing SRIOV configuration on default ethernet interfaces. This issue is now resolved.	4.3.2.230207	4.3.2.230270
CSCwh34432	While mounting vMedia using Redfish API, when the user forgets to post the **TransferProtocolType** field, the following error message is displayed: `Message: Bad request format` This issue is now resolved.	4.3.1.230097	4.3.2.230270
CSCwf44478	In Cisco UCS C-series M7 servers with Red Hat Enterprise Linux OS versions 8.6 and 9.0, Micron 7450 NVMe drive does not get detected after hot-plug. This issue is now resolved.	4.3.2.230207	4.3.2.230270

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwh13701	When Cisco UCS C225 M6 and C245 M6 servers, equipped with Liteon PSUs and have firmware versions prior to 4.2(3h), the servers will power off with no warning. This issue is now resolved.	4.3.1.230097	4.3.2.230270
CSCwh14449	When Cisco IMC is reset to factory default on Cisco UCS C220 M7 and C240 M7 server, the default admin password cannot be set using Redfish interface. This issue is now resolved.	4.3.2.230207	4.3.2.230270
CSCwf94278	In Cisco UCS C-series M5 servers with Cisco IMC release versions 4.1(3b), 4.2(2a), 4.2(3b), the user can create a session with a 'read only' user, but unable to delete or log out from the session while using the Redfish API interface. This issue is now resolved.	4.2(2a)	4.3.2.230207
CSCwh06536	The links with SFP-10G-T-X are up on VIC 14xx series adapters from the VIC firmware version 5.2(2b). However, the links with SFP-10G-T-X on VIC 14xx series adapters are down after upgrading the VIC firmware version to 5.3.2.32 from the version 5.2(2b). This issue is now resolved.	4.2(3b)	4.3.2.230270

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwb82433	Cisco UCS C220 M5 servers, equipped with Cisco UCS VIC 1400 series adapter and have **Geneve** feature enabled, go offline after the Cisco UCS VIC adapters fail to respond. This issue is now resolved.	4.2(1d)	4.3.2.230270

Resolved Caveats in Release 4.3.2.230207

The following defects were resolved in Release 4.3.2.230207:

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwf18625	Few UCS-HD1T7K12N and UCS-HD2T7K12N running firmware version CN05 may experience timeouts and go offline. This issue is now resolved.	4.1(3j)	4.3.2.230207
CSCwe92151	In Cisco UCS 240 M6 and M7 servers, the host automatically changes from power OFF to ON state when some hard disk drives are inserted or initialized while performing any operation. This causes low level firmware update failure. This issue is now resolved.	4.2(1a)	4.3.2.230207
CSCwf27804	Incorrect values observed for the OID .1.3.6.1.4.1.9.9.719.1.45.8.1.14 for RAID 10, RAID 50 and RAID 60 configuration. This issue is now resolved.	4.2(2a)	4.3.2.230207

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwe28875	When there is one or more Intel E810 card installed on the server during upgrade, HUU might report firmware update failure for any Intel NIC adapters in the system. This issue is now resolved.	4.3.1.230097	4.3.2.230207
CSCwd90347	On hot removal or insertion of NVMe drive, the Redfish PCI inventory does not get updated. The same inventory is updated in other Cisco IMC interfaces (GUI or CLI). This issue is now resolved.	4.2(3b)	4.2(3d)
CSCvq53066	During auto-upgrade of firmware from Cisco UCS Manager 4.0(2d) or earlier releases to Cisco UCS Manager 4.0(4b) or later releases, the SAS controller firmware is not activated on an integrated rack server. This issue is resolved.	4.0(4a)	4.1(1d)
CSCvt78954	Windows 2019 server OS installation fails on Cisco UCS C125 servers equipped with Cisco boot optimized m.2 RAID controller. This issue is resolved.	4.1(1e)	4.2(1d)
CSCvv08931	On the Cisco UCS S3260 Storage Server, the Chassis profile association failed due to configuration issues such as `connection management-expander-inoperable` and `insufficient-resources`. This issue is resolved.	4.0(4h)	4.2(1d)

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)

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.`
		4.2(2a)	4.2(3b)

CSCwd90347	On hot removal or insertion of NVMe drive, the Redfish PCI inventory does not get updated. The sameinventory is updated in other Cisco IMC interfaces (GUI or CLI). This issue is now resolved.	4.2(3b)	4.2(3d)
CSCwe44891	The **Delete all vNICs** option in the Web UI deletes 6 vNICs only. This issue is now resolved.	4.3.1.230097	4.3.1.230124
CSCwe48853	After performing data sanitization, the USB devices connected to the rear USB ports do not work. This issue is now resolved.	4.3.1.230097	4.3.1.230124

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwe87764	In Cisco UCS M7 servers equipped with 128GB DIMMs, there might be a decrease in the performance of the CPU when the values of the voltage regulator is modified to enhance the system performance. This issue is now resolved.	4.3.1.230138	4.3.1.230138
CSCwf52657	In Cisco UCS C240 M7 servers equipped with GPU and the BIOS parameter **Enhanced CPU performance** set to **auto**, the voltage regulator settings are retained. This issue is now resolved.	4.3.1.230138	4.3.2.230207

Open Caveats

Open Caveats in Release 4.3.2.240002

The following defect is open in Release 4.3.2.240002:

Defect ID	Symptom	Workaround	First Affected Release
CSCwi40270	In a Cisco UCS C240 M7 server set with Riser 1 Slot 1 populated with Intel, Mellanox or any other non Cisco cards and Cisco UCS VIC adapter is populated in Riser 1 Slot 2, the Cisco UCS VIC adapter might not get IP after Cisco IMC reset factory default.	1. Reset Cisco IMC to factory default. 2. Set the NIC mode to Cisco Card mode.	4.3.2.240002

Open Caveats in Release 4.3.2.230207

The following defects are open in Release 4.3.2.230207:

Defect ID	Symptom	Workaround	First Affected Release
CSCwj06157	In Cisco UCS M7 servers equipped with the next generation Cisco Boot optimized M.2 Raid controller, the system fan is ramping up and down.	Ignore the fan noise as it has no impact on functionality. OR Perform the following steps to set the **Fan Control Policy** to **High Power**: **1.** In the **Navigation** pane, click the **Compute** menu. **2.** In the work pane, click the **Power Policies** tab. **3.** In the **Configured Fan Policy** area, select **High Power** from the **Fan Policy** drop-down list. **4.** Click **Save Changes**.	4.3.2.230207
CSCwc27609	When the server is equipped with one or more Intel® E810 25G/100G Ethernet adapters attached to PCIe Gen5 riser, and the server is under continuous reboot, the Intel E810 25G or 100G adapter might not initialize on the PCIe bus.	Perform a DC power cycle to the servers. This re-initializes the adapter's PCIe interface.	4.3.1.230097
CSCwb55301	When VMD is enabled on Cisco UCS C240 M7 server equipped with 20 or more NVMe drives, the server might exhibit longer boot time (POST). This could be 1-2 minutes longer than in a server when VMD is disabled.	There are no known workarounds.	4.3.1.230097

Defect ID	Symptom	Workaround	First Affected Release
CSCvy26147	In a Cisco UCS C240 M6 server with dual UCSC-SAS-M6T card configured in legacy boot mode, drives in MRAID1 are not listed in Legacy OPROM dispatch after the link is disabled.	After replacing the adapters, ensure that the host is powered off and on. Reboot only with both the controller inserted.	4.2(1a)
CSCwb87912	When KMIP Client private key with size higher than 12 KB is used in Web UI, modify controller security operation times out in Web UI.	Use the private key size of 8 KB and refresh the Web UI after 2 minutes.	4.2(2a)
CSCwh14449	After Cisco IMC is reset to factory default on Cisco UCS C220 M7 and C240 M7 servers, the default admin password can not be set using Redfish API interface.	Use other Cisco IMC interfaces like Web UI, CLI, XML API and Cisco IMC configuration utility (F8) to set the admin password.	4.3.1.230097
CSCwf71163	When SRIOV is configured on non default ethernet interfaces and the host is rebooted, SRIOV configuration is not available on default interfaces. Configuring SRIOV on non default interfaces and rebooting the host might affect the existing SRIOV configuration on default ethernet interfaces.	Use SRIOV on only default interfaces.	4.3.2.230207
CSCwf44478	In Cisco UCS M7 C-series equipped with RHEL OS versions 8.6 and 9.0, Micron 7450 NVMe drive does not get detected after hot-plug.	• For RHEL 8.6 OS, update kernel to version 4.18.0-425.13.1.el8_7 or later. • For RHEL 9.0, update kernel to version 5.14.0-162.6.1.el9_1 or later.	4.3.2.230207

Defect ID	Symptom	Workaround	First Affected Release
CSCwf53294	In Cisco UCS M7 C-series with Cisco UCS release version 4.3.2.230207, unable to boot to RHEL 8.7 when VMD is enabled in the BIOS. the system boots to a blank screen or the system boot halts with an error message.	For a clean deployment, install RHEL 8.8. For existing RHEL 8.7 installations, perform the following steps: 1. Upgrade the kernel to 4.18.0-425.13.1.el8_7 or later. 2. Remove boot parameter intremap=off, if used before 3. Update BIOS to 4.3.2.230207. System should be able to boot to RHEL 8.7. For new RHEL 8.7 installation with 4.3.2.230207, perform the following steps: 1. Disable VMD. 2. Install RHEl 8.7. 3. Update kernel to 4.18.0-425.13.1.el8_7 or later. Reboot and enable VMD in the BIOS.	4.3.2.230207

Known Behaviors and Limitations in Release 4.3.2

Known Behaviors and Limitations in Release 4.3.2.230207

The following caveats are known limitations in release 4.3.2.230207:

Table 12: BMC

Defect ID	Symptom	Workaround	First Affected Release
CSCwf88782	When VIC firmware FPGA changes after firmware upgrade, VIC details might not be displayed in Cisco IMC.	Reboot the server as FPGA requires additional power cycle for the firmware to be updated.	4.3.2.230207
CSCwc59562	In Cisco IMC Web UI, CPU and Memory utilization percentage numbers might not match with the Operating System Utilization numbers.	There are no known workarounds.	4.3.1.230097
CSCvy26147	In a Cisco UCS C240 M6 server with dual UCSC-SAS-M6T card configured in legacy boot mode, drives in MRAID1 are not listed in Legacy OPROM dispatch after the link is disabled.	After replacing the adapters, ensure that the host is powered off and on. Reboot only with both the controller inserted.	4.2(1a)

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 modeswitches to Dedicated mode. Reboot the host again and enter the F8 utility to configure the network settings.	4.2(1c)
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)

Security Fixes in Release 4.3.2

Security Fixes in Release 4.3.2.240002

Defect ID - CSCwh68315

Cisco UCS M6 servers are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- **CVE-2023-23583**—Sequence of processor instructions leads to unexpected behavior in some Intel(R) processors and may allow an authenticated user to potentially enable escalation of privilege and information disclosure and denial of service through local access.

Defect ID - CSCwh23927

Cisco UCS C225 M6 and C245 M6 servers with AMD CPUs are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID:

- **CVE-2023-20569**—A side channel vulnerability on some of the AMD CPUs may allow an attacker to influence the return address prediction. This may result in speculative execution at an attacker-controlled address, potentially leading to information disclosure.

Defect ID - CSCwh43415

Cisco UCS C225 M6 and C245 M6 servers with AMD CPUs are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- **CVE-2021-26345**—Failure to validate the value in APCB may allow a privileged attacker to tamper with the APCB token to force an out-of-bounds memory read potentially resulting in a denial of service.
- **CVE-2022-23830**—SMM configuration may not be immutable, as intended, when SNP is enabled resulting in a potential limited loss of guest memory integrity.
- **CVE-2021-46774**—Insufficient DRAM address validation in System Management Unit (SMU) may allow an attacker to read/write from/to an invalid DRAM address, potentially resulting in denial-of-service.
- **CVE-2023-20519**—A Use-After-Free vulnerability in the management of an SNP guest context page may allow a malicious hypervisor to masquerade as the guest's migration agent resulting in a potential loss of guest integrity.
- **CVE-2023-20566**—Improper address validation in ASP with SNP enabled may potentially allow an attacker to compromise guest memory integrity.

Security Fixes in Release 4.3.2.230270

Defect ID - CSCwh17053

Cisco UCS C225 and C245 M6 servers are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- **CVE-2023-20593**—An issue in Zen 2 CPUs, under specific microarchitectural circumstances, might allow an attacker to potentially access sensitive information.

Defect ID - CSCwh18140

Cisco UCS C125 M5 servers are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- **CVE-2023-20593**—An issue in Zen 2 CPUs, under specific microarchitectural circumstances, might allow an attacker to potentially access sensitive information.

Security Fixes in Release 4.3.2.230207

Defect ID - CSCwe96259

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

- **CVE-2023-20228**—A vulnerability in the web-based management interface of Cisco Integrated Management Controller (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 - CSCwf29777

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

- **CVE-2019-11358**—jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.
- **CVE-2015-9251**—jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.

Defect ID - CSCwf30460

Cisco UCS M6 C-series servers are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- **CVE-2022-41804**—Unauthorized error injection in Intel(R) SGX or Intel(R) TDX for some Intel(R) Xeon(R) Processors which may allow a privileged user to potentially enable escalation of privilege through local access.
- **CVE-2022-40982**—Information exposure through microarchitectural state after transient execution in certain vector execution units for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure through local access.
- **CVE-2023-23908**—Improper access control in some 3rd Generation Intel(R) Xeon(R) Scalable processors may allow a privileged user to potentially enable information disclosure through local access.
- **CVE-2022-37343**— Improper access control in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege through local access.

Defect ID - CSCwf30468

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

- **CVE-2022-40982**—Information exposure through microarchitectural state after transient execution in certain vector execution units for some Intel(R) 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(R) Processors may allow a privileged user to potentially enable denial of service through local access.

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