Release Notes for Cisco UCS Rack Server Software, Release 3.0(4)

First Published: 2018-03-21

Last Modified: 2021-04-21

Cisco UCS C-Series and S-Series Servers

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

About the Release Notes

This document describes the new features, system requirements, open caveats and known behaviors for C-Series and S-Series software release 3.0(4) including Cisco Integrated Management Controller software and any related BIOS, firmware, or drivers. Use this document in conjunction with the documents listed in the Related Documentation section.

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

Support for Web UI Interface on Cisco UCS M3 Rack Server Software Post Flash Deprecation

The Cisco Cloud and Compute organization at Cisco expects that the Web UI interface of UCS M3 Standalone Rack Server Software – Cisco IMC – will not be accessible on future versions of web browsers that are going to deprecate support for Flash Player based content.

Cisco started shipping UCS C-Series and S-Series M3 Servers in 2012 and announced in 2015 and 2016 the EOL of all M3 rack server models, before Adobe announced the EOL of Flash Player support in July 2017. While we will continue to provide applicable service and support such as critical security fixes via patch releases for M3 servers through the End of Support date in December 2021, we do not plan to retrofit UCS C-Series and S-Series M3 platforms with HTML5-based Web UI interface for Cisco IMC.

Impacted customers can consider below alternatives for managing their M3 Rack Servers:

1. Use CLI interface of IMC Software to control and configure the standalone M3 rack platforms
2. Use a web browser that will not be deprecating support for Flash
3. Keep web browser on the last version that supports Flash and disable update to future version in order to continue using Web UI to manage M3 rack servers
4. Attach the M3 rack servers to Fabric Interconnects in order to use HTML5-based Web UI interface of a corresponding UCS Manager release

5. Access vKVM through the XML API in case Web UI is not available

Revision History

Revision	Date	Description
P1	April 21, 2021	Following changes were made: • Updated the Resolved Caveats section.
P0	February 22, 2021	Following changes were made: • Updated the Supported Software Features section. • Updated the HUU versions to 3.0(4s). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 3.0
M1	September 25, 2020	Added notice: *Support for Web UI Interface on Cisco UCS M3 Rack Server Software Post Flash Deprecation*
N0	August 14, 2020	Following changes were made: • Updated the Known Limitations and Behaviors section. • Updated the HUU versions to 3.0(4r). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 3.0

Revision	Date	Description
M0	June 4, 2020	Following changes were made: • Updated the Resolved Caveats section. • Updated the Known Behaviors section. • Updated the HUU versions to 3.0(4q). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 3.0
L0	April 20, 2020	Following changes were made: • Updated the Resolved Caveats section. • Updated the Open Caveats section. • Updated the HUU versions to 3.0(4p). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 3.0
K0	December 09, 2019	Following changes were made: • Updated the Resolved Caveats section. • Updated the Security Fixes section. • Updated the HUU versions to 3.0(4o). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 3.0

Revision	Date	Description
J0	September 17, 2019	Following changes were made: • Updated the Resolved Caveats section. • Updated the Security Fixes section. • Updated the HUU versions to 3.0(4n). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 3.0
I0	August 13, 2019	Following changes were made: • Updated the Resolved Caveats section. • Updated the HUU versions to 3.0(4m). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 3.0
H0	May 15, 2019	Following changes were made: • Updated the Resolved Caveats section. • Updated the HUU versions to 3.0(4l). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 3.0

Revision	Date	Description
G0	April 08, 2019	Following changes were made: • Security fixes were applied in this release. • Updated the Resolved Caveats section. • Updated the Supported Software Features section. • Updated the HUU versions to 3.0(4k). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 3.0

F0	September 10, 2018	Following changes were made:
		• Updated the Resolved Caveats section.
		• Updated the Open Caveats section.
		• Updated the HUU versions to 3.0(4j). Firmware for the following hardware was updated:
		  • Intel® SSD DC S4500 and DC S4600 Series SATA
		  • Micron 5100 SATA SSD (M.2 and U.2)
		  • Intel® SSD DC P4500 and P4600 Series NVMe
		The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 3.0

E0	August 29, 2018	Updated the Security Fixes for Release 3.0(4e) and Release 3.0(4i).

Revision	Date	Description
D0	July 20, 2018	Following changes were made: • Updated the Resolved Caveats section. • Updated the Security Fixes section. • Updated the HUU versions to 3.0(4i). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 3.0
C0	June 25, 2018	Following changes were made: • Updated the Resolved Caveats section. • Updated the Security Fixes section. • Updated the Supported Software Features section. • Updated the HUU versions to 3.0(4e). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 3.0

Revision	Date	Description
B0	May 10, 2018	Following changes were made: • A manufacturing issue was addressed in this release. • Updated the Supported Hardware section. • Updated the Resolved Caveats section. • Updated the HUU versions to 3.0(4d). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 3.0
A0	March 21, 2018	Created release notes for Release 3.0(4a).

Supported Platforms and Release Compatibility Matrix

Supported Platforms in this Release

The following servers are supported in this release:

- UCS-C22 M3
- UCS-C24 M3
- UCS-C220 M3
- UCS-C240 M3
- UCS-C3160 M3
- UCS-S3260 M3
- UCS-S3260 M4
- UCS-C220 M4
- UCS-C240 M4
- UCS-C460 M4

Cisco IMC and Cisco UCS Manager Release Compatibility Matrix

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

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

Table 1: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 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
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

Cisco IMC Release	Cisco UCS Manager Release	Rack-Mount Servers
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 2: 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
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 3: 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 4: 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
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

Cisco IMC Release	UCS Manager Release	Rack Mount Servers
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

System Requirements

The management client must meet or exceed the following minimum system requirements:

- Sun JRE 1.8.0_92 or later (Till 1.8.0_121)
- HTML based interfaces are supported on:
  - Microsoft Internet Explorer 10.0 or 11
  - Mozilla Firefox 30 or higher
  - Google Chrome 38 or higher
  - Safari 7 or higher

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

- For Classic View - all browsers must have Adobe Flash Player 11 plug-in or higher. Supported browsers are:
  - Microsoft Internet Explorer 11 or higher
  - Mozilla Firefox 54 or higher
  - Google Chrome 61 or higher
  - Safari 11 or higher
- Microsoft Windows 7, Microsoft Windows XP, Microsoft Windows Vista, Microsoft Windows 10, Apple Mac OS X v10.6, Red Hat Enterprise Linux 5.0 or higher operating systems
- Transport Layer Security (TLS) version 1.2.

Hardware and Software Interoperability

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

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

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

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

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

Upgrade Paths for Release 3.0

The section provides information on the upgrade paths for release 3.0. Refer to the table for upgrade paths for various Cisco UCS C-series IMC versions.

Table 5: Upgrade Paths to Release 3.0

Upgrade From Release	Upgrade To Release	Recommended Upgrade Path
Incase of C460 M4 for release lesser than 2.0(4c)	3.0	Follow these steps to upgrade from releases less than 2.0(4c) to 3.0: **Upgrade from version less than 2.0(4c) to 2.0(4c)** • You can use Interactive HUU or Non-Interactive HUU (NIHHU) script to update the server. • While updating the firmware using the Non-Interactive HUU (NIHUU) tool, use the Python scripts that are released with version 3.0(3a). • Use OpenSSL 1.0.0-fips on the client side (where the NIHUU python scripts are running). • Download HUU iso from here. • Download NIHUU script from here. **Upgrade from 2.0(4c) to 3.0** • You can use Interactive HUU or Non-Interactive HUU (NIHHU) script to update the server. • While updating the firmware using the Non-Interactive HUU (NIHUU) tool, use the Python scripts that are released with version 3.0(3a). • Use OpenSSL 1.0.1e-fips on the client side (where the NIHUU python scripts are running). • If you wish to secure Cimc Boot, set flag **use_cimc_secure** as **yes** in **multiserver_config** file present with python script. • Download HUU iso from here. • Download NIHUU script from here.

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

Upgrade From Release	Upgrade To Release	Recommended Upgrade Path
For C220 M4 and C240 M4 from 2.0	3.0(4a) and 3.0(4d)	Follow below upgrade path: • You can use Interactive HUU or Non-Interactive HUU (NIHHU) script to update the server. • While updating the firmware using the Non-Interactive HUU (NIHUU) tool, use the Python scripts that are released with version 3.0(3a). • Use OpenSSL 1.0.1e-fips on the client side (where the NIHUU python scripts are running). • If you wish to secure Cimc Boot, set flag **use_cimc_secure** as **yes** in **multiserver_config** file present with python script. • You must update the Cisco IMC (BMC) firmware twice. You must perform this double firmware update if you want to enable the device connector used with Cisco Intersight. • Interactive HUU takes care automatically, however you need to launch KVM and press HUU EXIT after second update to activate the same. That is, HUU updates CIMC first, activates and then KVM disconnects. Second update takes care of all updates of components including **CIMC -> Launch KVM again -> Exit HUU**. • Download HUU iso from here. • Download NIHUU script from here.

Upgrade From Release	Upgrade To Release	Recommended Upgrade Path
For M3 servers from 1.4 and releases lesser than 1.5(4)	3.0	**Before update, Reboot the bmc.** **Upgrade from 1.4 to 1.5(4)** • Use Interactive HUU, Non-Interactive HUU (NIHUU) script not supported for release 1.4 • Download HUU iso from Cisco.com **Upgrade from 1.5(4) to 2.0(4c)** • You can use Interactive HUU or Non-Interactive HUU (NIHHU) script to update the server. • While updating the firmware using the Non-Interactive HUU (NIHUU) script, use the Python scripts that are released with version 3.0(3a). • Use OpenSSL 1.0.0-fips on the client side (where the NIHUU python scripts are running). • Download HUU iso from here. • Download NIHUU script from here. **Upgrade from 2.0(4c) to 3.0** • You can use Interactive HUU or Non-Interactive HUU (NIHHU) script to update the server. • While updating the firmware using the Non-Interactive HUU (NIHUU) tool, use the Python scripts that are released with version 3.0(3a). • Use OpenSSL 1.0.1e-fips on the client side (where the NIHUU python scripts are running). • If you wish to secure Cimc Boot, set flag **use_cimc_secure** as **yes** in **multiserver_config** file present with python script • Download HUU iso from here. • Download NIHUU script from here.

Upgrade From Release	Upgrade To Release	Recommended Upgrade Path
For all M3 servers for releases after 1.5(4)	3.0	**Upgrade from 1.5 to 2.0(4c)** • You can use Interactive HUU or Non-Interactive HUU (NIHHU) script to update the server. • While updating the firmware using the Non-Interactive HUU (NIHUU) script, use the Python scripts that are released with version 3.0(3a). • Use OpenSSL 1.0.0-fips on the client side (where the NIHUU python scripts are running). • Download HUU iso from here. • Download NIHUU script from here. **Upgrade from 2.0(4c) to 3.0** • You can use Interactive HUU or Non-Interactive HUU (NIHHU) script to update the server. • While updating the firmware using the Non-Interactive HUU (NIHUU) tool, use the Python scripts that are released with version 3.0(3a). • Use OpenSSL 1.0.1e-fips on the client side (where the NIHUU python scripts are running). • If you wish to secure Cimc Boot, set flag **use_cimc_secure** as **yes** in **multiserver_config** file present with python script • Download HUU iso from here. • Download NIHUU script from here.

Firmware Upgrade Details

Firmware Files

The C-Series software release 3.0(4) includes the following software files:

CCO Software Type	File name(s)	Comment

Unified Computing System (UCS) Server Firmware	ucs-s3260-huu-3.0.4.iso ucs-c3160-huu-3.0.4.iso ucs-c240m4-huu-3.0.4.iso ucs-c220m4-huu-3.0.4.iso ucs-c460m4-huu-3.0.4.iso ucs-c220-huu-3.0.4.iso ucs-c240-huu-3.0.4.iso ucs-c2x-huu-3.0.4.iso For release specific ISO versions, see Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 3.0	Host Upgrade Utility
Unified Computing System (UCS) Drivers	ucs-cxxx-drivers.3.0.4.iso	Drivers
Unified Computing System (UCS) Utilities	ucs-cxxx-utils-efi.3.0.4.iso ucs-cxxx-utils-linux.3.0.4.iso ucs-cxxx-utils-vmware.3.0.4.iso ucs-cxxx-utils-windows.3.0.4.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 or CMC), since this could lead to unexpected behavior. If you choose to upgrade BIOS, the Cisco IMC and the CMC individually and not from the HUU ISO, make sure to upgrade both Cisco IMC, BIOS and CMC to the same container release. If the BIOS, CMC 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, CMC 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 3.1

Updating the Firmware

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

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

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

Note

- Downgrading a server from Cisco IMC version 3.0(x) to 2.0(x) resets the local admin password to the factory default password. After the downgrade is complete, you must manually change the password back to what was previously configured.
- We recommend that you use the **Update All** option from the Host Upgrade Utility to update the firmware versions of Cisco IMC, BIOS and all other server components (VIC, RAID Controllers, PCI devices, and LOM) together. Click **Exit** once you deploy the firmware.

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

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

Supported Features

Supported Hardware

Release 3.0(4d)

The following new hardware was added in release 3.0(4d):

- Artesyn 1050W Power Supply Unit support was added for the C3160 M3 and S3260 M3 servers.
- Intel ® SSD DC S4500 Series 480GB (UCS-SD480GBIS6-EV)
- Intel ® SSD DC S4500 Series 960GB (UCS-SD960GBIS6-EV)
- Intel ® SSD DC S4500 Series 3.8TB (CS-SD38TBIS6-EV)

Supported Software Features

Release 3.0(4s)

Following new PIDs are added:

PID	Server
UCS-SD16TSASS3-EP	Cisco UCS C220 M3 and C240 M3
UCS-SD32TSASS3-EP	Cisco UCS C220 M3 and C240 M3
UCS-C3K-3XTSSD16	Cisco UCS C3160 M3 and S3260 M4
UCS-C3K-3XTSSD32	Cisco UCS C3160 M3 and S3260 M4

Release 3.0(4k)

The following new software feature was added in Release 3.0(4k):

- An option to enable or disable **Challenge Password** while generating a Certificate Signing Request (CSR).

Release 3.0(4a)

The following new software features are supported in Release 3.0(4a):

- **Device Connector**—Enabling Cisco intersight management establishes a bi-directional communication between the cloud-based management platform and Cisco IMC. With this feature C220 M4,C240 M4 and C460 M4 systems can be monitored and inventoried from Cisco Intersight. This is an opt-out feature. If intersight management is not preferred then intersight can be turned OFF.

Note While upgrading from a previous version to the 3.0(4a) - 3.0(4d) versions, you must perform a double update of the Cisco IMC (BMC) firmware, if you want to enable the device connector used with Cisco Intersight. If not, while trying to access, a blank Intersight Device Connector screen may appear.

Important: In Release 3.0(4e), the issue of having to perform the upgrade twice to access the Cisco Intersight device connector has been addressed. With a single update you should be able to access the Cisco Intersight feature.

Software Utilities

The following standard utilities are available:

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

The utilities features are as follows:

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

SNMP

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

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

Note The above link is incompatible with IE 9.0.

Security Fixes

Security Fixes in Release 3.0(4o)

The following Security Fixes were added in Release 3.0(4o):

Release	Defect ID	CVE	Symptom
3.0(4o)	CSCvr54416	• CVE-2019-0151 • CVE-2019-11137	Cisco UCS C-Series and S-Series M4 servers that are based on Intel® processors are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs: • CVE-2019-0151 (CPU Local Privilege Escalation Advisory) affects certain Intel® 4th Generation Intel® Core™ Processors, 5th Generation Intel® Core™ Processors, 6th Generation Intel® Cores Processors, 7th Generation Intel® Core™ Processors, 8th Generation Intel® Core™ Processors, Intel® Xeon® Processors E3 v2/v3/v4/v5/v6 Family, Intel® Xeon® Processors E5 v3/v4 Family, Intel® Xeon® Processors E7 v3/v4 Family, Intel® Xeon® Scalable Processors 2nd Generation, Intel® Xeon® Scalable Processors, Intel® Xeon® Processors D-1500/D-2100), Intel® Xeon® Processors E-2100/E3100, and, Intel® Xeon® Processors W-2100/W-3100 when insufficient memory protection in Intel® TXT may allow a privileged user to potentially enable escalation of privilege through local access. This could result in bypassing Intel® TXT protections. • CVE-2019-11137 (BIOS 2019.2 IPU Advisory) affects 2nd Generation Intel® Xeon® Scalable Processors, Intel® Xeon® Scalable Processors, Intel® Xeon® Processor D Family, Intel® Xeon® Processor E5 v4 Family, Intel® Xeon® Processor E7 v4 Family, Intel® Atom® Processor C Series when insufficient input validation in the system firmware may allow a privileged user to potentially enable an escalation of privilege, denial of service, or information disclosure through local access. This release includes BIOS revisions for Cisco UCS M4 generation servers. These BIOS revisions include the updated microcode and Secure Initialization (SINIT) Authenticated Code Modules (ACM) for Cisco UCS M4 servers, which are required part of the mitigation for these vulnerabilities.

Release	Defect ID	CVE	Symptom
3.0(4o)	CSCvr54416	• CVE-2019-0151	Cisco UCS C-Series and S-Series M3 servers that are based on Intel® processors are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs: • CVE-2019-0151 (CPU Local Privilege Escalation Advisory) affects certain Intel® 4th Generation Intel® Core™ Processors, 5th Generation Intel® Core™ Processors, 6th Generation Intel® Cores Processors, 7th Generation Intel® Core™ Processors, 8th Generation Intel® Core™ Processors, Intel® Xeon® Processors E3 v2/v3/v4/v5/v6 Family, Intel® Xeon® Processors E5 v3/v4 Family, Intel® Xeon® Processors E7 v3/v4 Family, Intel® Xeon® Scalable Processors 2nd Generation, Intel® Xeon® Scalable Processors, Intel® Xeon® Processors D-1500/D-2100), Intel® Xeon® Processors E-2100/E3100, and, Intel® Xeon® Processors W-2100/W-3100 when insufficient memory protection in Intel® TXT may allow a privileged user to potentially enable escalation of privilege through local access. This could result in bypassing Intel® TXT protections. This release includes BIOS revisions for Cisco UCS M3 generation servers. These BIOS revisions include the updated Secure Initialization (SINIT) Authenticated Code Modules (ACM) for Cisco UCS M3 servers, which are required part of the mitigation for these vulnerabilities.

Security Fixes in Release 3.0(4n)

The following Security Fixes were added in Release 3.0(4n):

Release	Defect ID	CVE	Symptom
3.0(4n)	CSCvp34795	• CVE-2018-12126 • CVE-2018-12127 • CVE-2018-12130 • CVE-2019-11091	Cisco UCS C-Series and S-Series M3 servers that are based on Intel® Xeon® Processor E5 v2 processors are vulnerable to variants of exploits that use Microarchitectural Data Sampling (MDS) to gain access to data being processed in the CPU by other applications. • CVE-2018-12126 (Microarchitectural Store Buffer Data Sampling) affects store buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Cisco IMC release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. • CVE-2018-12127 (Microarchitectural Load Port Data Sampling) affects load buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Cisco IMC release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. • CVE-2018-12130 (Microarchitectural Fill Buffer Data Sampling) affects line fill buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Cisco IMC release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. • CVE-2019-11091 (Microarchitectural Uncacheable Data Sampling) affects the uncacheable memory buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Cisco IMC release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. This release includes BIOS revisions for Cisco UCS M3 generation servers. These BIOS revisions include the updated microcode that is a required part of the mitigation for these vulnerabilities.

Security Fixes in Release 3.0(4l)

The following Security Fixes were added in Release 3.0(4l):

Release	Defect ID	CVE	Symptom
3.0(4l)	CSCvp34790 CSCvp34799	• CVE-2018-12126 • CVE-2018-12127 • CVE-2018-12130 • CVE-2019-11091	Cisco UCS C-Series and S-Series M4 servers are based on Intel® Xeon® Processor E7 v2, v3, and v4 Product Family processors that are vulnerable to variants of exploits that use Microarchitectural Data Sampling (MDS) to gain access to data being processed in the CPU by other applications. • CVE-2018-12126 (Microarchitectural Store Buffer Data Sampling) affects store buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Cisco IMC release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. • CVE-2018-12127 (Microarchitectural Load Port Data Sampling) affects load buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Cisco IMC release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. • CVE-2018-12130 (Microarchitectural Fill Buffer Data Sampling) affects line fill buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Cisco IMC release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. • CVE-2019-11091 (Microarchitectural Uncacheable Data Sampling) affects the uncacheable memory buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Cisco IMC release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. This release includes BIOS revisions for Cisco UCS M4 generation servers. These BIOS revisions include the updated microcode that is a required part of the mitigation for these vulnerabilities.

Release	Defect ID	CVE	Symptom
3.0(4l)	CSCvp34786	• CVE-2018-12126 • CVE-2018-12127 • CVE-2018-12130 • CVE-2019-11091	Cisco UCS C-Series and S-Series M4 servers are based on Intel® Xeon® Processor E5 v3 and v4 Product Family processors that are vulnerable to variants of exploits that use Microarchitectural Data Sampling (MDS) to gain access to data being processed in the CPU by other applications. • CVE-2018-12126 (Microarchitectural Store Buffer Data Sampling) affects store buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Cisco IMC release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. • CVE-2018-12127 (Microarchitectural Load Port Data Sampling) affects load buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Cisco IMC release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. • CVE-2018-12130 (Microarchitectural Fill Buffer Data Sampling) affects line fill buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Cisco IMC release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. • CVE-2019-11091 (Microarchitectural Uncacheable Data Sampling) affects the uncacheable memory buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Cisco IMC release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. This release includes BIOS revisions for Cisco UCS M4 generation servers. These BIOS revisions include the updated microcode that is a required part of the mitigation for these vulnerabilities.

Security Fixes in Release 3.0(4i)

The following Security Fixes were added in Release 3.0(4i):

Release	Defect ID	CVE	Symptom
3.0(4i)	CSCvm03357	• CVE-2018-3615 • CVE-2018-3620 • CVE-2018-3646	Cisco UCS C-Series M3 servers are based on Intel® processors that are vulnerable to exploits that use CPU speculative processing and data cache timing to potentially identify privileged information. These exploits are collectively known as L1 Terminal Fault (L1TF). • CVE-2018-3615 (affecting SGX), also known as Foreshadow, is not known to affect any existing Cisco UCS servers because Cisco UCS M5 and earlier generation servers, and HyperFlex M5 and earlier generation servers do not use Intel® SGX technology. • CVE-2018-3620 (affecting OS/System Management Mode) and CVE-2018-3646 (affecting Virtual Machine Monitors) are referred to as L1 Terminal Fault attacks by Intel®. These vulnerabilities are mitigated by applying the updated processor microcode from Intel® included in the server firmware bundle, and the relevant Operating System and Hypervisor patches from the appropriate vendors. This release includes BIOS revisions for Cisco UCS M3 generation servers. These BIOS revisions include the updated processor microcode that is a required part of the mitigation for CVE-2018-3620 (OS/SMM) and CVE-2018-3646 (VMM). Operating System and Hypervisor patches from the appropriate vendors may also be required to mitigate these vulnerabilities. For more information, please see the Cisco Security Advisory at: CPU Side-Channel Information Disclosure Vulnerabilities: August 2018

Release	Defect ID	CVE	Symptom
3.0(4i)	CSCvj59326	• CVE-2018-3639 • CVE-2018-3640	Cisco UCS C-Servers M4 servers are based on Intel® processors that are vulnerable to variants of an exploit that uses CPU speculative processing and data cache timing to efficiently leak information, known as Spectre. CVE-2018-3639 (Spectre/Variant #4) and CVE-2018-3640 (Spectre/Variant #3a) are addressed by applying the updated processor microcode from Intel included in the server firmware bundle, and the relevant Operating System and Hypervisor patches from the appropriate vendors. This release includes BIOS revisions for Cisco UCS M4 generation servers. These BIOS revisions include the updated processor microcode that is a required part of the mitigation for CVE-2018-3639 (Spectre/Variant #4) and CVE-2018-3640 (Spectre/Variant #3a).
3.0(4i)	CSCvj59312	• CVE-2018-3639 • CVE-2018-3640	Cisco UCS C-Servers M3 servers are based on Intel® processors that are vulnerable to variants of an exploit that uses CPU speculative processing and data cache timing to efficiently leak information, known as Spectre. CVE-2018-3639 (Spectre/Variant #4) and CVE-2018-3640 (Spectre/Variant #3a) are addressed by applying the updated processor microcode from Intel included in the server firmware bundle, and the relevant Operating System and Hypervisor patches from the appropriate vendors. This release includes BIOS revisions for Cisco UCS M3 generation servers. These BIOS revisions include the updated processor microcode that is a required part of the mitigation for CVE-2018-3639 (Spectre/Variant #4) and CVE-2018-3640 (Spectre/Variant #3a).

Security Fixes in Release 3.0(4e)

The following Security Fixes were added in Release 3.0(4e):

Release	Defect ID	CVE	Symptom
3.0(4e)	CSCvm03353	• CVE-2018-3615 • CVE-2018-3620 • CVE-2018-3646	Cisco UCS C-Series M4 (except C460 M4) servers are based on Intel® processors that are vulnerable to exploits that use CPU speculative processing and data cache timing to potentially identify privileged information. These exploits are collectively known as L1 Terminal Fault (L1TF). • CVE-2018-3615 (affecting SGX), also known as Foreshadow, is not known to affect any existing Cisco UCS servers because Cisco UCS M5 and earlier generation servers, and HyperFlex M5 and earlier generation servers do not use Intel® SGX technology. • CVE-2018-3620 (affecting OS/System Management Mode) and CVE-2018-3646 (affecting Virtual Machine Monitors) are referred to as L1 Terminal Fault attacks by Intel®. These vulnerabilities are mitigated by applying the updated processor microcode from Intel® included in the server firmware bundle, and the relevant Operating System and Hypervisor patches from the appropriate vendors. This release includes BIOS revisions for Cisco UCS M4 (except 460 M4) generation servers. These BIOS revisions include the updated processor microcode that is a required part of the mitigation for CVE-2018-3620 (OS/SMM) and CVE-2018-3646 (VMM). Operating System and Hypervisor patches from the appropriate vendors may also be required to mitigate these vulnerabilities. For more information, please see the Cisco Security Advisory at: CPU Side-Channel Information Disclosure Vulnerabilities: August 2018

Release	Defect ID	CVE	Symptom
3.0(4e)	CSCvj59318	• CVE-2018-3639 • CVE-2018-3640	Cisco UCS C-Servers M4 servers are based on Intel® processors that are vulnerable to variants of an exploit that uses CPU speculative processing and data cache timing to efficiently leak information, known as Spectre. CVE-2018-3639 (Spectre/Variant #4) and CVE-2018-3640 (Spectre/Variant #3a) are addressed by applying the updated processor microcode from Intel included in the server firmware bundle, and the relevant Operating System and Hypervisor patches from the appropriate vendors. This release includes BIOS revisions for Cisco UCS M4 generation servers. These BIOS revisions include the updated processor microcode that is a required part of the mitigation for CVE-2018-3639 (Spectre/Variant #4) and CVE-2018-3640 (Spectre/Variant #3a).

Security Fixes in Release 3.0(4a):

The following Security Fixes were added in Release 3.0(4a):

Release	Defect ID	CVE	Symptom
3.0(4a)	CSCvh07357	CVE ID not available for this fix	A vulnerability in the web interface of the Cisco UCS C-Series Rack Servers related to Clickjacking or Phishing attack is addressed.

Release	Defect ID	CVE	Symptom
3.0(4a)	CSCvg97965, CSCvg97979, CSCvg98015	• CVE-2017-5715 • CVE-2017-5753 • CVE-2017-5754	Cisco UCS C-Series servers are based on Intel processors that are vulnerable to exploits that use CPU speculative processing and data cache timing to potentially identify privileged information. These exploits are collectively known as Spectre and Meltdown. • CVE-2017-5753 Spectre/Variant 1 – is addressed by applying relevant Operating System and Hypervisor patches from the appropriate vendors. • CVE-2017-5715 Spectre/Variant 2 – is addressed by applying the updated microcode included in the UCS C-Series release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. • CVE-2017-5754 Meltdown – is addressed by applying the relevant operating system patches from the appropriate vendors. This UCS C-Series release includes the BIOS revisions for Cisco UCS M4 and M3 generation servers that includes the updated microcode that is a required part of the mitigation for CVE-2017-5715 (Spectre/Variant 2). For more information, please see the Cisco Security Advisory at: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180104-cpusidechannel

Resolved Caveats

The following section lists resolved caveats.

Resolved Caveats in Release 3.0(4)

Release 3.0(4s)

The following defect is resolved in Release 3.0(4s):

Table 6: BMC

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvw96906	When you login to the CIMC with valid username and invalid password, the username is not included in the audit message.	3.0(4s)	3.0(4s)

Release 3.0(4q)

The following defects are resolved in Release 3.0(4q):

Table 7: VIC Firmware

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvm59040	Cisco UCS C220 servers with an up-time of over 180 days and equipped with Cisco UCS VIC 1225 may report loss of connectivity from the host. This issue is now resolved with the latest firmware version.	2.0(13f)	3.0(4q)

Release 3.0(4p)

The following defects are resolved in Release 3.0(4p):

Table 8: External Controllers

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvt63509	The following LT0400MO and LT1600MO SSD models report 0GB of available storage space remaining under normal operating conditions for forty thousand power on hours: • UCS-SD400G1KHY-EP • UCS-SD400G12S4-EP • UCS-C3X60-12G240 • UCS-SD16TG1KHY-EP • UCS-SD16TB12S4-EP • UCS-C3X60-12G2160 The drives go offline and become unusable after a power-cycle. This issue is now resolved with the latest firmware version.	3.0(4p)	3.0(4p)

Release 3.0(4o)

The following defects are resolved in Release 3.0(4o):

Table 9: External Controllers

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvr67027	Cisco UCS S3260 M4 servers did not recognize boot drivers after upgrading from RHEL 7.6 to 7.7 version. This issue is now resolved.	3.0(1d)	3.0(4o)

Release 3.0(4n)

The following defects are resolved in Release 3.0(4n):

Table 10: BMC

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvq57969	Vulnerability scanner indicates missing X-XSS-Protection header despite being present.	3.0(4a)	3.0(4n)

Table 11: External Controller

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvj91628	LSI 9271 encounters a fatal firmware (FW) error. All the file systems on the RAID controller will go offline or be disconnected.	3.0(4a)	3.0(4n)

Release 3.0(4m)

The following defect is resolved in release 3.0(4m):

Table 12: BMC

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvq83392	Added support for new upgrade or downgrade rules for Adopter BU.	3.0(4l)	3.0(4m)

Release 3.0(4l)

The following defect is resolved in release 3.0(4l):

Table 13: BMC

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvp41543	SSH clients fail to establish a connection to Cisco IMC. This happens when the SSH clients use `diffie-hellman-group14-sha1` as default KEX algorithm as support for this KEX algorithm has been removed from Cisco IMC. Update the SSH clients to the latest version that uses stricter KEX algorithms to establish SSH sessions.	3.0(4j)	3.0(4l)

Release 3.0(4k)

The following defects are resolved in release 3.0(4k):

Table 14: BMC

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvm37559	Following HTTP headers were missing in the HTTP response for TCP port 80 and TCP port 443: • X-Content-Type-Options • X-XSS-Protection	3.0(2f)	3.0(4k)

Release 3.0(4j)

The following defects are resolved in release 3.0(4j):

Table 15: BMC

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCve60056	After upgrading the C-Series servers to 3.0(x) firmware versions, SNMP does not return the correct local disk status.	3.0(1d)	3.0(4j)
CSCvk52168	On the S3260 servers, when you use SLAAC to launch the KVM or Cisco IMC web UI, the BMC SLAAC IP is unresponsive to pings.	3.0(4i)	3.0(4j)

Release 3.0(4i)

The following defects are resolved in release 3.0(4i):

Table 16: Host Firmware Upgrade

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvk17568	Unable to launch non-interactive HUU while using IPv6 NFS share. The following error appears: `"Error: Bad remote share specification or Server not reachable"`	3.0(4a)	3.0(4i)

Table 17: Hardware

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvj83780	Under specific low write and long idle time workloads, the following SATA SSDs no longer show read errors: • UCS-M2-240GB • HX-M2-240GB	3.0(4a)	3.0(4i)

Release 3.0(4e)

The following defects are resolved in release 3.0(4e):

Table 18: BMC

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvj66524	On Cisco IMC of an S3260 server, a **BIOS POST Timeout** error may be displayed for even though the server is booted and running without issues.	3.0(1c)	3.0(4e)

Table 19: Web Management

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvj42923	Unable to launch the KVM window when you use the IPv6 address and the IPv4 address is not set or set to 0.0.0.0.	3.0(3a)	3.0(4e)

Table 20: XML API

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvj75669	On the S3260 servers, you cannot set BMC2 Interface using the XML API when only one compute node is present.	3.0(4a)	3.0(4e)

Release 3.0(4d)

The following defects are resolved in release 3.0(4d):

Table 21: BMC

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvj54481	In the Redfish schema, reset action under Systems is incorrectly named as "**System.Reset**" instead of "**ComputerSystem.Reset**" and also "**Target**" is incorrect, it should have been "**target**". These two are not in compliant with the Redfish schema.	3.0(4a)	3.0(4d)
CSCvi06813	Fans intermittently spin and return to normal speed after a short time. This happens due to a failure to read the sensors on the raid controller within the timeout value.	3.0(3b)	3.0(4d)
CSCvi92466	When a user password has the '**$**' (dollar sign), **export-vnic** command fails to export the vNIC configuration using the ftp protocol.	3.0(3a)	3.0(4d)

Release 3.0(4a)

The following defects are resolved in release 3.0(4a):

Table 22: BMC

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvh61997	C240 M4 SD boot (Raid 1) server, after upgrading to version 3.0(3e) fills up the obfl and messages log with following message (this fills up the syslog): `4:2018 Jan 3 18:03:05 CET:BMC:kernel:-:<4>CYWB FWLOG (usbapp): USB VendorAck event, data=04:2018 Jan 3 18:04:10 CET:BMC:kernel:-:last message repeated 5 times.....`	3.0(3a)	3.0(4a)
CSCvh66273	Cisco IMC reboot is required to raise a fault for a predictive failure on a drive.	3.0(3f)	3.0(4a)

Table 23: External Controllers

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvg25428	Call Home Alert messages are being generated regularly (once in a week).	3.0(3f)	3.0(4a)

Open Caveats

The following section lists open caveats.

Open Caveats in Release 3.0(4)

Open Caveats in Release 3.0(4p)

The following defect is open in release 3.0(4p):

Table 24: Host Firmware Upgrade

Defect ID	Symptom	Workaround	First Affected Release
CSCvt79547	In Cisco UCS C220 M3 servers, Interactive HUU automatically triggers the activation after completing the updates, without waiting for the user to press **EXIT**.	This issue does not have any functionality impact. All the components are updated and successfully activated.	3.0(4o)

Open Caveats in Release 3.0(4l)

The following defect is open in release 3.0(4l):

Table 25: BIOS

Defect ID	Symptom	Workaround	First Affected Release
CSCvo77732	After upgrading the C460 M4 servers with Intel® Xeon® Processor v2 to 4.0(1a) version, server encounters a CATERR fault and the server becomes unresponsive.	Downgrade to 3.0(x) version.	3.0(4a)

Open Caveats in Release 3.0(4j)

The following defect is open in release 3.0(4j):

Table 26: BIOS

Defect ID	Symptom	Workaround	First Affected Release
CSCvm41493	On the C460M4 servers with Intel X710 or XL710 adapters, firmware version of the Intel 710 PCIe adapters displays 0 in the Cisco IMC web UI.	None.	3.0(4j)

Open Caveats in Release 3.0(4a)

The following defect is open in release 3.0(4a):

Table 27: Web Management

Defect ID	Symptom	Workaround	First Affected Release

CSCvj37231	SMTP stops sending mail alerts after Cisco IMC is upgraded to 3.0(4a) version.	Upgrade Cisco IMC to 3.0(4d) and use CLI to configure .
		`Server # scope smtp`
		`Server /smtp # set from-addr Server@cisco.com`
		`Server /smtp *# commit`
		Note We recommend that you add an unique Hostname in the From address field so that the address is clearly distinguished.
		For example, all the mails send would have the From address as "C240M4-FXX1836J72S@cisco.com
			3.0(4a)

Open Caveats in Release 3.0(3)

Open Caveats in Release 3.0(3e)

The following defects are open in release 3.0(3e):

Table 28: PID

Defect ID	Symptom	Workaround	First Affected Release
CSCvg05613	PID information of the following drives is not reported correctly: • UCS-S3260-NVM48 • UCS-S3260-NVM416 • UCS-S3260-NVM464 • UCS-S3260-NVM432	Power off the host and update the CMC with the latest S3260 PID catalog.	3.0(3e)

Open Caveats in Release 3.0(3a)

The following defects are open in release 3.0(3a):

Table 29: BIOS

Defect ID	Symptom	Workaround	First Affected Release
CSCvb11910	M3 servers may become unresponsive during system BIOS POST at the 'Configuring platform Hardware' stage with a CATERR error in the system event log.	Enable the Fault Resilient Booting (FRB) timeout for an automatic recovery.	3.0(3a)

Table 30: BMC

Defect ID	Symptom	Workaround	First Affected Release
CSCvd84866	On the S3260 server with dual controllers, when you hot swap all of the physical drives (56) without AC cycle or rebooting the host, the old physical drive data continues to remain in the web UI and PMCLI. This only happens on systems where all the 56 drives are present, and multiple virtual drives are configured.	Toggle the server's blade power.	3.0(3a)
CSCvb89330	On the C460 M4 servers, when you downgrade firmware using NI-HUU to any 2.x release firmware, multiple fan sensor failure events are observed momentarily. This might occur after you manually power cycle the server post the update.	None.	3.0(3a)

Table 31: External Controllers

Defect ID	Symptom	Workaround	First Affected Release
CSCvd54828	The RAID controller encounters an error and resets. This happens when you use an external SATA solid state drive (SSD) and not an SAS SSD.	None.	3.0(3a)
CSCuv67943	On the C3160 server, the MSM Application displays a pop-up message reporting a defective slot. However, the error is displayed for one slot number below it. For instance, if slot number 31 is a defective slot, the error displays slot 30 as the defective slot.	Add a single number to the error message to view the correct slot number.	3.0(3a)

Defect ID	Symptom	Workaround	First Affected Release
CSCva90939	On the S3260 server, the physical and logical sectors of physical drives in a MegaRAID Storage Manager (MSM) are shown incorrectly when drives are unzoned from one server and rezoned onto another server on the S3260 server node configurations.	Refresh the MegaRAID Storage Manager (MSM) screen. This displays the physical drive information correctly. Alternatively, you can use the Cisco IMC storage page to view the physical drive's physical and logical information.	3.0(3a)
CSCvd25263	In rare situations, the Cisco 12G SAS Modular RAID Controller may encounter a multi-bit ECC error during sustained heavy IO load.	Replace the controller with a new one and return the old controller.	3.0(3a)
CSCvd07355	On the S3260 servers, enabling or disabling connection management results in unpredictable I/O performance. This happens when the host is online.	Move the host offline before enabling or disabling connection management.	3.0(3a)
CSCvd18495	On the C460 M4 server downgrading the firmware on the 10GE LOM port (X540 based) from release 3.0(3) to an earlier release fails and the following error message is displayed: *ERROR LOM Firmware EEupdation failed (Error Code: 2705)*	None.	3.0(3a)
CSCvd10359	Downgrading the firmware version of the Intel X540 PCIe adapter from 3.0(3) version to any previous versions fails and HUU displays the following failure message: *Intel X540 PCI adapter update failed (Error Code: 3115)*	None	3.0(3a)

Table 32: Hardware

Defect ID	Symptom	Workaround	First Affected Release
CSCvc17387	On some C220 M4 servers using a 770 watt power supply unit (PSU) and attached to a UPS, a PSU error is displayed when you upgrade the firmware to release 2.0(13e). The error might occur as a result of noise generated by the UPS.	None.	3.0(3a)

Table 33: Utilities

Defect ID	Symptom	Workaround	First Affected Release
CSCvd78351	While trying to perform a Cisco IMC configuration import using the UCSCFG utility, importing Cisco IMC data fails and an import failure message is displayed. This happens when the power characterization status is running or if it is required to be run.	Run power characterization manually before importing or exporting the Cisco IMC configuration.	3.0(3a)

Open Caveats in Release 3.0(2b)

The following defects are open in release 3.0(2b):

Table 34: BMC

Defect ID	Symptom	Workaround	First Affected Release
CSCvc31545	You cannot configure KMIP setting using Cisco IMC Import or Export options.	Manually configure the KMIP setting on each server using XML API, web UI, CLI.	3.0(2b)

Open Caveats in Release 3.0(1c)

The following defects are open in release 3.0(1c):

Table 35: BMC

Defect ID	Symptom	Workaround	First Affected Release
CSCvb49288	In the web UI, when the field **Percentage Life left** shows a percentage of below 35%, the status bar is displayed in red, but no fault engine entry is generated.	None. The **Percentage Life Left** field in the UI just represents an advisory warning.	3.0(1c)

Table 36: External Controllers

Defect ID	Symptom	Workaround	First Affected Release
CSCvb96598	After upgrading the server to release 3.0(1x), when you try to re-insert a boot device using the 'CTRL-C' utility on the SAS HBA controller, the default add key '+' does not function as expected. The **Boot Order** field accepts a value or 0 or 1, which indicates the presence of multiple controllers. However, currently, you are unable to modify or enter a value in the field. This happens when you upgrade from previous releases such as release 2.0(10) or 2.0(13).	Use the '**INS**' key instead of the default '+' key in the CTRL-C utility to re-insert the boot device.	3.0(1c)

Table 37: Utilities

Defect ID	Symptom	Workaround	First Affected Release
CSCvc25435	HDD firmware continues to show an older version after an upgrade using the host update utility. This happens if you change the firmware to AHCI mode in the advanced BIOS settings. As a result the firmware activation fails.	Upgrade the firmware in the LSI SW RAID mode.	3.0(1c)

Open Caveat in Release 2.0(13h)

The following defect is open in release 2.0(13h):

Table 38: Cisco IMC

Defect ID	Symptom	Workaround	First Affected Release

CSCva96401	On the C220 M4 and C240 M4 servers, installed with 1227, 1387 or 1385 VIC adapters, intermittently, upon rebooting the server, the VIC adapters get mapped out. **Note** The VIC adapter is rediscovered in a subsequent host reboot.	None.	2.0(13h)

Open Caveats in Release 2.0(13e)

The following defects are open in release 2.0(13e):

Table 39: BIOS

Defect ID	Symptom	Workaround	First Affected Release
CSCva38014	On the C220 M4 and C240 M4 servers, the system could become unresponsive during BIOS posting, at the 'Configuring and Memory' stage, and logs the following warning: `A warning has been logged! Warning Code = 0x30, Minor Warning Code = 0x13, Data = 0x10100`	1. AC power off the server 2. Unplug the cable 3. Swap the CPUs 4. Re-seat the DIMMs and then power the server back on.	2.0(13e)
CSCuz94596	DIMMs are mapped out while testing the reboot process. This issue occurs only when Intel Xeon v4 processors and Montage DIMMs are used, where the DIMM round trip time is greater than expected for the DIMM.	None.	2.0(13e)

Table 40: External Controllers

Defect ID	Symptom	Workaround	First Affected Release

CSCva82566	The Intel X520 network adapter may not display the vNIC path in the web UI or command line interface after service profile association.	None.	2.0(13e)
CSCuy16602	Resetting the storage controller during an ongoing I/O operation results in a BSOD.	None.	2.0(13e)
CSCuy37152	On the C220 M4 server, the OMB drive is not marked Bad by the Cisco UCSC-P-12Gbps SAS HBA controller after it fails discovery.	None.	2.0(13e)
CSCuz21377	On the C240 M4 servers, the Web UI and command line interface display only one connector display view (CN0) in the expander attached cases.	See the storage logs and watch out for these strings: • BBBBBBBB000 0000000000000 • BBBB0000000 0000000000000	2.0(13e)
CSCva59776	On the C240 M4 servers, a recently inserted drive's LED blinks even when another drive is issued a Locate LED command. This is observed with any operation with consecutive Locate LED commands, after a drive has been inserted.	Note down the physical slot of drive before performing drive removal operation.	2.0(13e)
CSCvb00471	Windows OS crashes with a Blue Screen Of Death due to heavy IO. Multi-bit ECC errors found in the logs.	None.	2.0(13e)

Open Caveats in Release 2.0(9c)

The following defects are open in release 2.0(9c):

Table 41: VIC

Defect ID	Symptom	Workaround	First Affected Release

CSCuw17399	When you check the transceiver details after an active optical cable of length seven meters is connected from the Cisco UCS VIC 1387 adapter to a Nexus 3016Q switch, it fails to detect the QSFP type. When we check the transceiver details, it does not detect the QSFP type of connector.	None.	2.0(9c)

Open Caveats in Release 2.0(4c)

The following defects are open in release 2.0(4c):

Table 42: BIOS

Defect ID	Symptom	Workaround	First Affected Release
CSCut37666	In the JBOD mode, after creating the precision boot order for the HDDs connected to the Cisco 12G Modular SAS Pass through controller, the HDDs do not appear in the created order. This issue applies to LSI controllers with JBOD capability.	Use F6/Setup Boot order control for controlling the System boot order	2.0(4c)

Table 43: HUU

Defect ID	Symptom	Workaround	First Affected Release
CSCus94537	HDD firmware update using HUU takes time as the HDD firmware is updated sequentially. This increases the time to upgrade a server which has many HDD	None	2.0(3d)

Open Caveats in Release 2.0(3d)

The following defects are open in release 2.0(3d):

Table 44: BIOS

Defect ID	Symptom	Workaround	First Affected Release

CSCup56423	Actual boot order does not have the information to identify which LUN is assigned to LSI sSATA, LSI SATA, and different HDDs in AHCI mode.	Set the ROM mode option to UEFI only.	2.0(3d)
CSCun24358	C220 M4 and C240 M4 servers do not reboot on pressing F10 after changing the adapter settings using HII interface from BIOS setup. The servers continues to boot and the new settings do not take effect.	Manually reboot the servers.	2.0(3d)

Open Caveats in Release 1.4(7)

The following defects are open in release 1.4(7):

Table 45: CIMC

Defect ID	Symptom	Workaround	First Affected Release
CSCud18756	LSI storage controllers with external ports (-8e cards) do not show up in CIMC local storage management.	None.	1.4(7)

Known Behaviors

The following section lists known behaviors.

Known Limitations and Behaviors in Release 3.0(4)

Known Limitations and Behaviors in Release 3.0(4r)

Table 46: BMC

Defect ID	Symptom	Workaround	First Affected Release
CSCvt12298	If SNMP is enabled in Cisco UCS C220 M3 servers, then firmware upgrade through HUU or NIHUU fails with the following error message: `Not enough memory, Please reboot CIMC`		3.0(4q)

Defect ID	Symptom	Workaround	First Affected Release
		Perform the following steps: **1.** Power off the server. **2.** Reboot Cisco IMC. **3.** In the **Navigation** pane, click the **Compute** menu. **4.** In the work pane, click the **Remote Management** tab. **5.** Under **Virtual KVM**, click **Launch vKVM**. **6.** In the **vKVM console**, go to **Virtual Media** > **Create Image**. **7.** Navigate to and select the ISO file and click **Open** to mount the image. **8.** Go to **Power** > **Power Cycle System (cold boot)**. **9.** Press **F6** when the server starts to select a boot device. **10.** Use the arrow keys to select Cisco Virtual CD/DVD and then press **Enter**. **11.** Once fully loaded and scanned, upgrade only Cisco IMC. Ignore any system warning. **12.** • If Cisco IMC updates successfully, update	

Defect ID	Symptom	Workaround	First Affected Release
		everything else. • If you still get the same error, select the option to reboot. Wait for 10-15 minutes and reconnect to Cisco IMC and vKVM. **13.** Try to upgrade only Cisco IMC again. Ignore any system warning. In case the above steps do not resolve the issue, perform the following additional steps: Reboot Cisco IMC and disable SNMP before upgrading the firmware. Enable SNMP after upgrading the firmware.	

Known Limitations and Behaviors in Release 3.0(4q)

The following are the known behaviors in release 3.0(4q):

Table 47: External Controllers

Defect ID	Symptom	Workaround	First Affected Release
CSCvu41958	Firmware update of Emulex cards LPe16002, OCe14102, and OCe11102 cards from any release earlier than 2.0(13q) to the latest release may fail.	Upgrade path: **1.** Upgrade to release 2.0(13q). **2.** Upgrade to latest release.	3.0(4p)

Defect ID	Symptom	Workaround	First Affected Release
CSCvu42509	User is unable to configure FC and FCoE LUN on Cisco UCS C-Series M3 servers equipped with LPe16002 and OCe11102 cards. The target details for mapping LUN on the server side in card BIOS does not populate.	There is no known workaround for this issue. You should use either LPe16002 card or OCe11102 card in the same server in order to configure FC and FCoE LUN.	3.0(4p)

Known Behaviors in Release 3.0(3)

Known Behaviors in Release 3.0(3e)

The following are the known behaviors in release 3.0(3e):

Table 48: External Controllers

Defect ID	Symptom	Workaround	First Affected Release
CSCvf96879	Activation of HTML based vMedia fails. This happens when you use Google Chrome browser versions 61 or 62.	Use IE or any other browser.	3.0(3a)

Known Behaviors in Release 3.0(3a)

The following are the known behaviors in release 3.0(3a):

Table 49: BIOS

Defect ID	Symptom	Workaround	First Affected Release
CSCuq15528	In the legacy boot mode, a few boot options do not appear in the menu or boot override page. This is an intermittent issue and happens when there are multiple boot options with SATA/RAID connected and UEFI boot options are disabled in the boot options.	If you want to boot from a particular option which does not appear on the menu or the override options, run the policy from Cisco IMC, or press F2 and set the device as the first boot device. All the devices will be listed correctly on the boot options page.	3.0(3a)

CSCva57433	The Intel Ethernet Converged Network Adapter X710-DA2 PCI Card is unable to launch the legacy iSCSI option ROM for Port 2. You can view this by searching the SEL log for the warning message: `Not enough memory available to shadow a legacy option ROM.` This happens when the system is configured for legacy boot, and the Intel Ethernet Converged Network Adapter X710-DA2 PCI Card is configured to the iSCSI boot. The card consumes extra runtime Option ROM memory space, and is able to load the Option ROM for only Port 1. Once the Option ROM for Port 1 is loaded, the remaining available Option ROM memory space is insufficient to load the Option ROM for Port 2.	Use Port 1 for the legacy iSCSI boot with the X710-DA2 PCI card and disable the Option ROM for the rest of the slots and the LOMs.	2.0(13e)

Table 50: BMC

Defect ID	Symptom	Workaround	First Affected Release
CSCux43338	On the Mozilla Firefox web browser 42.0, when you click the **Paste Server Certificate** option on the Web UI, the pop-up dialog box eclipses the **Save Certificate** and **Cancel** buttons.	Move the dialog box so as to make the **Save Certificate** and **Cancel** buttons visible, or use a different web browser such as Google Chrome or Microsoft Internet Explorer.	2.0(9c)
CSCuw76431	While installing Red Hat Enterprise Linux 7.1 operating system on the UCS C-Series servers, a critical SEL entry similar to this is created: *The 2015-10-12 10:35:07 critical "System Software event: OS Event sensor, unknown event".*	None.	2.0(9c)

CSCvd04304	When you perform reset to factory defaults after configuring the KMIP certificates and KMIP server details, the existing Cisco IMC and KMIP server certificates are not deleted as expected.	Scope into any kmip mode in the command line interface and use the **restore** or **delete** command. Alternatively, log on to the web UI and use the **Delete** button on the **Secure Key Management** tab.	3.0(3a)

Table 51: External Controllers

Defect ID	Symptom	Workaround	First Affected Release
CSCvc51343	C220 M4 and C240 M4 servers with Broadcom 5709 Ethernet PCIe Adapter may crash after heavy network utilization.	Disable Active State Power Management (ASPM) for PCI devices in BIOS.	3.0(3a)
CSCuy05774	On the S3260 server, when you attempt to shut down the server on the RedHat Linux OS 7.2, by default the OS boots to the web UI mode (Ctrl+Alt+F7), and the power shutdown command from BMC puts the system to sleep. Any action on the keyboard or the mouse brings the system back to life. The same behavior is observed when the user logs in as root.	Use the shell prompt interface (Ctrl+Alt+F2)and log in as root.	3.0(3a)
CSCvc81096	M3 or M4 servers are difficult to detect whenever the server is pulled out. M3 servers need an "S1" display for backward-compatibility since they cannot support multiple controllers, and M4 servers need an "S1-MZ1" display since these support multiple controllers. This happens when you configure zoning on the server and then pull the server out.	None.	3.0(3a)
CSCux20272	On the C240 M4 servers, Redhat Enterprise Linux OS version 6.5 fails to boot after installation. This happens when you install the OS using a PXE or DVD image.	During the OS installation, do not select the **Desktop Packages** option.	2.0(10b)
CSCva44733	When Option ROM is disabled in the PCI slot configuration, storelib library is unable to inventory the disks.	Keep the Option ROM enabled.	2.0(13e)

CSCvb34628	On rare occasions, while updating the firmware of the storage controller, it fails with a "Flash Programming error" resulting in a failed controller requiring Return Material Authorization (RMA). This only happens when the firmware update is issued while there is a battery super capacitor relearn in progress and the relearn completes before the flash write is complete.	If this issue occurs, do the following: 1. Check the status of the battery/super capacitor learn cycle and wait for it to complete. 2. Ensure that the "Next learn time" is not anytime in the next hour before issuing the firmware update.	2.0(13e)
CSCva55926	Redhat Enterprise Linux OS version 7.2 fails to install on Qlogic 8442T ISCSI LUN with an 'Unknown error occurred' message.	None.	2.0(13e)

Table 52: External OS

Defect ID	Symptom	Workaround	First Affected Release
CSCvd65151	RedHat Enterprise Linux operating system version 6.8 does not boot through the iSCSI LUN if you choose desktop packages during the OS installation. This happens only when the OS is installed in an iSCSI target, and not on a local storage or SAN target.	If desktop packages are mandatory for the installation, use RedHat Enterprise Linux operating system version 6.9.	3.0(3a)
CSCuz28948	On the C460-M4 servers, due to ESXi vFlash on the SSD LSI driver issue, the RedHat Enterprise Linux virtual machine crashes. This happens when several IOs are running with backup software.	Disable the vFlash.	3.0(3a)

Table 53: Utilities

Defect ID	Symptom	Workaround	First Affected Release
CSCvd34692	While trying to initiate a Delay firmware update using UCS Configuration Utility, NIHUU fails to trigger the update. This happens when you set the one-time boot order using KVM or web UI.	Cancel the request and set the one-time boot order using CLI.	3.0(3a)

Defect ID	Symptom	Workaround	First Affected Release
CSCvc78162	While configuring a boot order, when you enable IPv6 before exporting the Cisco IMC tokens to a text file (using the UCS CFG tool in Windows), the 'V6-Enabled' token is displayed as 'Disabled' even when IPv6 is displayed as enabled in Cisco IMC.	Use the web UI, command line interface or XML API interface to get the 'V6-enabled' token status back to 'Enabled'.	3.0(3a)
CSCvc78173	When you configure a boot order from the web UI use the set command to set the boot order, an error message 'class name tag missing' is displayed. This happens when you import the boot order to a text (input) file using the UEFI shell and the boot order help content is a part of the input file.	Delete the help content and retain the set parameter data in the input file.	3.0(3a)
CSCvc56345	On the S3260 servers, when you downgrade release 3.0(3) to an earlier version using the HUU, CMC1 and CMC2 fail to get activated. This happens when the single server dual SIOC function is enabled.	Disable the single server dual SIOC option before downgrading the server.	3.0(3a)

Table 54: VIC Firmware

Defect ID	Symptom	Workaround	First Affected Release
CSCuu59408	On the Nexus 7018 switch version 7.2.0 (where the fabric extender N2232PP uplink is connected to only one F2 Module port, and the host interface connected to the physical host UCS is shared with the storage virtual device), reloading the F2 module post the module uplink to the host interface results in the DCBX PDU acknowledgment getting lost.	In the owner virtual device of Nexus 7018 switch, flap the host interface (HIF) port of fabric extender so that the DCBX exchange is initialized.	2.0(6d)

Table 55: Web Management

Defect ID	Symptom	Workaround	First Affected Release
CSCvd58182	On the C220 M3, C240 M3, C22 M3 and C24 M3 servers, the Java based KVM fails to launch. This happens when you use Microsoft Internet Explorer browser with Java version 1.8 (update 121).	When the security warning pops up on your screen during the launch, click **Cancel**. The KVM console then launches successfully.	3.0(3a)

Known Behaviors in Release 3.0(1c)

The following are the known behaviors in release 3.0(1c):

Table 56: BIOS

Defect ID	Symptom	Workaround	First Affected Release
CSCva99738	You cannot save the BIOS setting changes using the BIOS option 'Save and Exit' when you are logged in with user privileges. This happens only when you log on to the BIOS setup area in the user mode.	Press the key F10 to save and exit.	3.0(1c)
CSCvc14144	When you update the BIOS with the Enhanced Intel Speedstep Technology (EIST) disabled during setup, power characterization fails to occur, and its status is displayed as 'Not Run'.	None.	3.0(1c)
CSCva67765	On the C460 M4 servers, after you change the VLAN settings using the Cisco IMC F8 configuration menu, the VLAN settings are correctly applied, but do not display completely on the configuration menu.	Wait for two minutes or more before pressing the **F5** button to refresh the screen.	2.0(13e)

Table 57: BMC

Defect ID	Symptom	Workaround	First Affected Release
CSCvb77846	When you launch the HTML based KVM on the Safari browser without installing the certificate properly, the HTML based KVM fails to launch.	Complete the following steps to install the certificate: 1. When the message 'Safari cannot verify the identity of the website XXXXX' is displayed, click the **Show Certificate** button. 2. From the certificate drop-down menu, select **Always Trust**. 3. Click **Continue**. You are prompted to enter your local password and update the certificate. 4. Click **Update Settings**. The certificate is installed. You may use this certificate for all communications with the server.	3.0(1c)
CSCva43470	Activating virtual media on the HTML based KVM consoles fails on the Mozilla Firefox browser version 32.0.	Use Mozilla Firefox browser version 38.0 or later, or use different browser such as Google Chrome or Microsoft Internet Explorer.	3.0(1c)
CSCva05249	Virtual Media data transfer on the HTML based KVM console takes a lot of time.	Use Java based virtual media with the encryption disabled.	3.0(1c)
CSCuy92283	LDAP user authentication fails when you download the CA Chain certificate to Cisco IMC, and certificate binding is enabled.	Convert the CA Chain certificate, which is in the .p7b format, to the PEM format before downloading to Cisco IMC.	2.0(13e)
CSCuz82915	When Redhat Linux is in the UI mode, and you enable the scroll key, it is not displayed on the HTML KVM window.	None. Scroll lock is not supported by Redhat in the UI mode.	2.0(13e)

Table 58: External Controllers

Defect ID	Symptom	Workaround	First Affected Release

CSCvc08224	Updating the HDD firmware on VMware operating systems using the PMCSSACLI utility fails when you enter the command: `pmcssacli ctrl slot=1 pd CN0:1:1 flash file=firmware.bin mode=7 immediate=enable`. The firmware update is successful only if you use a forced flag in the command. This happens because a remote connection environment between the server or client SSACLI does not support command prompts in VMware.	Use a force flag option as shown in the example: `pmcssacli ctrl slot=1 pd CN0:1:1 flash file=firmware.bin mode=7 immediate=enable forced`.	3.0(1c)

Table 59: Utilities

Defect ID	Symptom	Workaround	First Affected Release

CSCvc06814	The latest non-interactive HUU Python script fails to retrieve cookies and update the firmware components in Release 3.0(1).	Follow these guidelines to resolve the issue:
		• If you are upgrading from a release older than release 2.0(3):
		  • Use the Open SSL Version 1.0.0-fips on the client, and upgrade to release 2.0(4) release first using the python script available in release 2.0(4).
		  • Use the Open SSL 1.0.1e-fips on the client, and upgrade to release 3.0(1) using the python script available in release 3.0(1).
		• If you are upgrading the firmware from release 2.0(2) and later to release 3.0(1), use the Open SSL 1.0.1e-fips, and update to 3.0(1) using the NIHUU python scripts available in release 3.0(1).
		• If you are downgrading from 3.0(1) to any 2.0 release to 2.0(1), use the Open SSL 1.0.1e-fips on the client and downgrade to the required version.
			3.0(1c)

CSCvc38739	After updating firmware using the non-interactive HUU script, the firmware output summary occasionally displays a timeout error such as this: `Firmware update failed for CIMC - <IP>, Error - Firmware update failed because it timed out. Check host for details.` Despite the error message, the firmware update might be successful.	Check whether or not all firmware components are updated successfully.	3.0(1c)

Table 60: VMware

Defect ID	Symptom	Workaround	First Affected Release
CSCux87650	On servers with VMware ESXi 5.5.0 or later, the storecli is able to identify the adapter but unable to communicate with the storage controller.	Disable the affected module from the ESXi command line and use the following command to communicate with the controller: 1. `esxcli system module set --enabled=false --module=lsi_mr3` 2. `~# esxcli system module set --enabled=false --module=lsi_mr3` 3. `~# reboot`	2.0(10b)

Table 61: Web Management

Defect ID	Symptom	Workaround	First Affected Release
CSCvb78527	When you log on to Cisco IMC using Microsoft Internet Explorer and click the **Help** button, the page prompts you to enable pop-up windows. After you enable the pop-up window and Internet Explorer reloads, the icons on the page are not displayed, and the Help window fails to open.	Use the Google Chrome or Mozilla Firefox browser.	3.0(1c)
CSCuz83739	On the HTML based KVM console, occasionally when you try to map an image in the virtual media using the drop and down method, the virtual media stops responding.	Use the Browse option to map the virtual media image.	3.0(1c)
CSCvb43134	After upgrading the firmware to 3.0(1) from a previous version, upon logging in for the first time, the page displays the old web UI instead of the new HTML5 based UI.	Refresh the web browser.	3.0(1c)

Defect ID	Symptom	Workaround	First Affected Release
CSCvb67922	A Native Library error is displayed when you launch the KVM console with multiple (pre-existing) Java versions.	Complete the following steps to disable multiple Java versions on your machine: 1. Select **Configure Java** in Start panel. 2. Click the **Java** tab. 3. Click **View**. 4. From the list of Java versions, uncheck the check boxes for the Java versions that you do not need, and check the version that is appropriate.	3.0(1c)
CSCvb66685	On the HTML based KVM console, the 'CTRL' and 'ALT' keys do not function.	Create user-define macros using the option Macro > Manage or use the Java based KVM.	3.0(1c)
CSCuz68208	Unable to maximize the HTML based KVM console to full-screen mode on the Microsoft Internet Explorer.	Use the Google Chrome or Mozilla Firefox browser.	3.0(1c)
CSCuz39581	You cannot launch a Java based KVM on a browser having Java 8 Update 77.	Use the latest Java version available, which is Java8 Update 92 or 91. Or use Java 8 Update 45 or below.	2.0(13e)

Table 62: XML API

Defect ID	Symptom	Workaround	First Affected Release
CSCvb17203	XML API operations using the commands CURL or POST in a web browser, in release 3.0, do not work with Transport Layer Security (TLS) versions 1.0 and 1.1.	Upgrade to TLS version 1.2.	3.0(1c)

Known Behaviors in Release 2.0(13e)

The following defects are known behaviors in release 2.0(13e):

Table 63: BIOS

Defect ID	Symptom	Workaround	First Affected Release

CSCux72847	PXE boot from second 10 GE LOM port does not work. This issue may occur when PXE boot is configured to boot from the second 10GE LOM port, and the SAS controller Option ROM is also enabled and loaded.	Disable the SAS or LOM0 (1GE) Option ROMs to free up enough space to load both the 10GE Option ROMs.	2.0(13e)
CSCuy15543	On the Cisco IMC Web UI and CLI the actual boot order is displayed incorrectly when you configure the **IpmiBootOrder** from Cisco IMC using the **Configpolicy.xml** file that is used to configure the precision boot order policy.	None. The incorrect boot order should be ignored. The functionality works as expected and the BIOS setup displays the actual boot order correctly.	2.0(9e)

Table 64: BMC

Defect ID	Symptom	Workaround	First Affected Release
CSCux92616	With the client system running Java version 1.8 and update 66, KVM crashes while trying to activate vMedia and accept the pop-up prompt for unencrypted vMedia session.	Enable virtual media encryption using the Cisco IMC Web UI to avoid this pop-up.	2.0(13e)

Table 65: External Controllers

Defect ID	Symptom	Workaround	First Affected Release
CSCuy62185	Unable to access the **Fast Utility** option by pressing the **`Ctrl+Q`** keys, when the port is configured with iSCSI.	Enable port 60/64 emulation under USB configuration in BIOS.	2.0(10b)
CSCuz55512	SLES11 SP3 OS legacy installation becomes unresponsive on the C220 M4 and C240 M4 servers with inbox drivers for UCSC-PSAS12GHBA.	None. Use async drivers.	2.0(13e)
CSCuy12854	All Drives except boot drives are marked as `Offline` by UCSC-PSAS12GHBA on Windows.	None.	2.0(13e)
CSCuv51716	The C240 M4 servers connected to a Magma Chassis GPU Expander with Multiple Tesla (k40/K80) cards and running RedHat Enterprise Linux 6.x operating system occasionally become unresponsive during a reboot.	Hard reboot the server.	2.0(9c)

CSCuw86750	When physical drives containing all virtual drives are removed or replaced, the system displays a fault "configuration lost" which remains unchanged until a virtual drive is created or the configuration is cleared using WebBIOS or Ctrl +R function.	Reboot to see if the error is cleared. In most cases, it gets cleared. If the error is not cleared, create a virtual drive or clear configuration using Web BIOS or the Ctrl+R function.	1.5(1)
CSCux44506	If a boot virtual drive is marked hidden after setting a different virtual drive as boot drive, and if the system is running from the previously configured boot virtual drive, the system may shut down based on the operating system.	None.	2.0(9c)
CSCuz61344	While trying to login into standalone Cisco IMC version 2.0.9 using CLI or GUI the interface becomes unresponsive. Sometimes an error is displayed, but most times it is unresponsive. Thsi happens due to LDAP group authorization in Cisco IMC.	Remove the affected LDAP group from the Group Authorization options or resolve the circular loops in the AD database. Modify search-group-depth to a value between 1-3.	2.0(9d)
CSCuz93611	When a Virtual Drive or a Drive Group is set to Transport Ready and a member physical drive is removed, the Virtual Drive or Drive Group cannot be deleted as it is blocked and also Transport Ready state cannot be cleared since Transport Ready is only for Optimal VD or DG.	Remove all members of the VD/DG and reinsert and then continue with next steps.	2.0(13e)
CSCva17225	Even after the **PowerSave** command has been sent to all the physical drives, Samsung and SanDisk SAS SSDs will remain active. This is because they do not support the Start Stop Unit (SSU) command.	None.	2.0(13e)
CSCuw55009	On the 3260 servers, while upgrading to or downgrading from SAS firmware supporting 240 VD firmware, these issues are seen: During an upgrade, *auto-rebuild* does not get initiated, and during a downgrade, consistency check and secure erase operations do not resume.	None.	2.0(9)

Table 66: Firmware Upgrade

Defect ID	Symptom	Workaround	First Affected Release
CSCuz48865	Unable to downgrade the host firmware from 2.0(13x) version to 2.0(2x) versions.	Downgrade the firmware from 2.0(13x) to 2.0(6f) first and then downgrade it to 2.0(2x) versions.	2.0(13e)

Table 67: LSI

Defect ID	Symptom	Workaround	First Affected Release
CSCun50408	Creating VD from StorCli and WebBIOS, the default disk policy shown after creation is inconsistent in different UI. MegaRAID Storage Manager shows Unchanged and StorCli shows "Disk's default"	None. Both Unchanged and Disk's Default means the same in this case. Cisco supported Drives have **disk cache policy = Disabled** so in this case the Disk's Default or Unchanged refer to the same indicating the Disk cache is disabled.	2.0(4c)

CSCuq35761	LSI applications such as StorCli and MSM and CIMC Storage management allows JBOD with Operating system or File system to be converted to Unconfigured Good drives without meaningful error message indicating there could be data loss in such cases.	Users should be aware that there is going to be data loss when JBOD which has OS or File system is converted to Unconfigured Good. LSI Applications like MSM and StorCli prompt users with "Are you sure" message so users need to be careful to understand there will be data loss in such cases if they chose to convert JBOD with OS or File system to Unconfigured good drives. CIMC storage management allows JBOD to be converted to Unconfigured Good without any Warning Pop-Up message. Again users need to be make sure that there is no OS or Filesystem when they choose to convert JBOD to Unconfigured Good drives.	2.0(4c)
CSCus82741	LSI SWRAID driver with RHEL displays "`Buffer IO Error`" in the `messages` file when RAID INIT operation is done.	None.	2.0(4c)

Table 68: XML API

Defect ID	Symptom	Workaround	First Affected Release
CSCva77821	Few components such as BIOS, BMC, CMC fail to get activated while upgrading from 2.0(7e) to 2.0(13e) using non-interactive HUU.	Upgrade from 2.0(7e) to 2.0(9l), then upgrade to 2.0(13e).	2.0(13e)

Known Behaviors in Release 2.0(12b)

Following is the known behavior for Release 2.0(12b):

Table 69: Cisco IMC

Defect ID	Symptom	Workaround	First Affected Release
CSCuz30387	On the C460 M4 servers, host serial port (PMCLI) does not work when the host is powered off.	Power on the host.	2.0(12b)

Known Behaviors in Release 2.0(10e)

Following is the known behavior for Release 2.0(10e):

Table 70: External Controllers

Defect ID	Symptom	Workaround	First Affected Release
CSCuy42320	If firmware is downgraded to legacy firmware, or Transport Ready is disabled in the new firmware, Transport Ready is cleared in NVRAM. But if the firmware is not a legacy firmware or it does not have Transport Ready implementation, Transport Ready is not cleared. In this case if Transport Ready aware firmware is flashed again, Transport Ready DGs will reappear. You are then required to manually clear Transport Ready.	None.	2.0(10b)
CSCux62038	When the Qlogic QLE8362 card is populated in the set-up, the server is unable to boot to BIOS (F2 menu).	Use Cisco IMC to configure all BIOS related settings.	2.0(10b)

Table 71: BIOS

Defect ID	Symptom	Workaround	First Affected Release
CSCuy46516	When connected to a Magma chassis with the K80 populated in the chassis, intermittently the server becomes unresponsive during a BIOS POST.	None.	2.0(10b)

Known Behaviors in Release 2.0(9d)

Following are the known behaviors for release 2.0(9d):

Table 72: External Controllers

Defect ID	Symptom	Workaround	First Affected Release
CSCuu56166	On the C3260 server, after you perform expansion or raid-level migration operations Virtual Drives (VD) do not display the updated size.	Complete the following steps: **1.** Unclaim the disk from usage by powering off all the virtual machines before running the following command: *~ esxcli storage core claiming unclaim ?t device ?d naa.xxx* **2.** Ensure that the file naa.xxx disk is not located under **/vmfs/devices/disks** **3.** Reclaim the disk again using the following command:*~ esxcli storage core adapter rescan ?A vmhbaX* **4.** Check whether or not the disk is added back with the new size.	2.0.7(d)

Known Behaviors in Release 2.0(9c)

Following are the known behaviors for release 2.0(9c)

Table 73: BMC

Defect ID	Symptom	Workaround	First Affected Release
CSCun99348	When virtual KVM is disabled, the **Play Recording** action on the **Troubleshooting** screen fails.	Enable **Virtual KVM** on the **Remote Presence** tab.	2.0(1)
CSCuv08978	Management port MTU cannot be configured due to hardware limitations.	None.	1.5(4)

CSCuj36245	After restoring to factory defaults, when you import the BIOS tokens on the target machine, the values remain unchanged.	Power on the target machine and try the import operation after the BIOS post is completed.	2.0(1)

Table 74: BIOS

Defect ID	Symptom	Workaround	First Affected Release
CSCun99297	Cannot select specific USB thumb drive under boot option priorities.	Use F6 from the boot selection menu to select specific USB drives.	2.0(1)
CSCuo08591	System becomes unresponsive in the POST after the SD card removal when the host is powered on.	**1.** AC cycle the system after removing the SD card. **2.** Reinsert the SD card.	2.0(4c)
CSCun91835	Boot order varies when enabling or disabling the Option ROM.	None.	2.0(1)
CSCur61234	In the secure boot mode, a security violation error is triggered. This issue could also occur while trying to perform an AC power cycle, when the power characterization is enabled in the UEFI secure mode.	None.	2.0(4)

Table 75: LSI

Defect ID	Symptom	Workaround	First Affected Release
CSCum87051	Random behavior of system freeze at boot @ BIOS POST screen for around 2 minutes followed by "Waiting for Battery Pack" message on LSI Ctrl-R BIOS for another 2 minutes. This only happens if there is a learn cycle pending for the supercap and the host is restarted (either AC/DC/reboot). At all other reboot/power cycle, this does not happen.	There is no work-around at this time.	2.0(4c)

CSCuu86314	On M4 servers, the iMR (Zero-memory) RAID Controller supports up to 32 virtual drives, but the command to create virtual drives in a single drive group allows only 16 virtual drives.	None. The RAID controller supports 32 virtual drives across all drive groups and only 16 drives in a single drive group.	2.0(6)
CSCum87232	Cisco IMC storage BBU info shows the Pack Energy value below the design capacity. This is also seen in the **storcli /cX /cv show all** command. On the current shipping 6G SAS RAID Controllers with Supercap, the Pack energy is always above the design capacity. This is a change in behavior confuses the user and makes the user think the supercap has or is going bad and gets a worrisome situation of the data integrity.	There is no work-around at this time. This is just a display issue and does not impact the actual functionality or data integrity.	2.0(4c)
CSCuw69844	On the servers with 2008M-8i, the VMware ESXi 5.5 Update 1 install fails while loading the installer.	**1.** Go to System BIOS (Press F2) **2.** Choose PCI configuration > MMCFG **3.** Change the value from Auto to 2 GB **4.** Change the value of Memory Mapped IO above 4G to Enabled **5.** Save and reboot the system.	2.0(7)

Table 76: External Controllers

Defect ID	Symptom	Workaround	First Affected Release

CSCuw42070	The MegaRAID Storage Manager fails to detect a new 6TB HGST drive with yellow amber LED. This happens when the drive is corrupted and displays an SAS link failure.	None.	2.0(8)
CSCuw55045	SAS Flash and MSM utilties are unable to downgrade the IT firmware if the Network Virtualization (NV) data version changes. To downgrade the NV data version, use the FlashOEM tool bundled with the Host Upgrade Utility (HUU).	Do not use SAS Flash and MSM utilities to downgrade the IT firmware. Use these to only use the HUU.	2.0(9c)
CSCuw09414	Powering off Virtual machines (VM) with the Virtual Graphics Processor unit (vGPU) takes 90 to 120 seconds in VMware ESXi 6.0.	Power off smaller number of VMs at one time.	2.0(4c)

Table 77: External OS

Defect ID	Symptom	Workaround	First Affected Release
CSCuw80507	According to the knowledge base at https://access.redhat.com/solutions/21322, using IPMI commands on the Red Hat Enterprise Linux results in the over use of CPU resources.	Add the following command at the end of the kernel line in /etc/grub.conf: *ipmi_si.kipmid_max_busy_us=<time in microseconds>*	1.5(2)

Known Behaviors in Release 2.0(8d)

Following are the known behaviors for release 2.0(8d):

Table 78: BMC

Defect ID	Symptom	Workaround	First Affected Release

CSCul16923	The fault code F0181 is raised by CIMC when the local disk is removed while the rack server was in use. This fault is visible through CIMC WebUI, CLI and SNMP interfaces. But the same fault is not retrievable through the XML API interface.	None.	1.5(4)
CSCuj40520	Upgrading firmware with Host Upgrade Utility (HUU) can cause temporary storage faults while the upgrade is in progress. These faults are benign and will clear once the upgrade is complete.	None.	1.5(4)

Table 79: Cisco IMC

Defect ID	Symptom	Workaround	First Affected Release
CSCuq23984	Cisco IMC does not respond during OOB update of utility virtual drives (SCU/HUU/Drivers) on flex flash.	It is recommended that host reboot actions are not performed while running OOB update of utility virtual drives on flex flash.	2.0(3d)

Table 80: Web Management

Defect ID	Symptom	Workaround	First Affected Release
CSCuv63101	User gets logged out of the Web UI occasionally, after upgrading the Cisco IMC firmware from 2.0(6) to 2.0(8). This happens when browser cookies are not cleared.	Clear the browser cookies.	2.0(7)

Table 81: BIOS

Defect ID	Symptom	Workaround	First Affected Release
CSCun00121	Cannot create boot option for partitions in SD card.	None.	2.0(1)

CSCul84767	The system locks up while running memtest86 from memtest.org. The problem is seen only with memtest86 from memtest.org.	Do no use memtest86 from memtest.org on C460 M4. Please use PassMark or any other memory test tools that have the support for IvyBridge EX platforms instead.	2.0(4c)
CSCun02543	Port number attributes are missing in the actual boot order for the FC and FCOE cards.	None.	2.0(1)

Table 82: External Controllers

Defect ID	Symptom	Workaround	First Affected Release
CSCut92393	On the C240 M4 servers, on rare occasions, the Cisco 12 Gigabyte SAS Modular RAID Controller displays an error when you try deleting a virtual drive.	None.	2.0(6)
CSCuv34371	When creating new virtual drives of any RAID type, the write cache policy defaults to 'write through' even with a fully functional BBU or super-capacitor battery. When a BBU is present, the default write cache policy should be 'write back with good BBU'. This happens on the C240 M4 and C220 M4 servers with 12 gigabyte SAS mezzanine RAID controllers.	In the standalone mode, on the Ciso IMC storage tab of the Web UI, edit the virtual drive to set the write caching policy to 'write back with good BBU'. You can also modify the setting using the LSI command line option **rom config utility** .	2.0(3d)
CSCuv36714	The MegaRAID Storage Manager displays consistency check errors on RAID 1 volume in Windows. This happens when you try writing data to the drive 20 to 30 minutes after a consistency check (which appears to be normal).	This is a known Microsoft limitation. For more information, see https://support.microsoft.com/en-us/kb/2713398	2.0(4c)

Table 83: External GPU Expanders

Defect ID	Symptom	Workaround	First Affected Release

CSCuv04922	On the C240 M4 server, A "PCI Resource Error" message is seen with the Magma Chassis GPU Expander configuration due to a CPU I/O space limitation which supports a maximum of 64K. This happens when all or some of the PCI slots are occupied by different third party adapters.		2.0(4c)

			For Nvidia Grid K1 configuration: (where one Nvidia Grid K1 is internally connected on the C240 M4, and two Nvidia Grid K1 adapters are externally connected through the Magma Chassis) • Local Boot: Cisco 12 Gigabyte SAS Modular RAID controller (HBA slot), Intel I350 LOM (L slot), Nvidia Grid K1 (slot2), Magma Expander HBA (slot5), Teradici APEX2800(slot6), Fusion IO drive(slot4) • iSCSI Boot: Intel i350 LOM (L slot), Nvidia Grid K1(slot2), Magma Expander HBA (slot5), Teradici APEX2800(slot6), Fusion IO drive(slot4) • SAN Boot: CISCO VIC1227(MLOM), Nvidia GRID K1 (slot2), Magma Expander HBA (slot5), Teradici APEX2800(slot6), Fusion IO drive(slot4) For Nvidia Grid K2 configuration: (where one Nvidia GridK2 is internally connected on the C240 M4, and four Nvidia Grid K2 adapters are externally connected through the Magma Chassis)		

		• Local Boot: CISCO 12G SAS Modular RAID controller (HBA slot),Intel I350 LOM (L slot), Nvidia GRID K2 (slot2), Magma Expander HBA (slot5), Teradici APEX2800(slot6), Fusion IO drive(slot4) • iSCSI Boot: Intel i350 LOM(L slot), Nvidia Grid K2 (slot2), Magma Expander HBA (slot5), Teradici APEX2800(slot6), Fusion IO drive(slot4) • SAN Boot: CISCO 1227 SAN (MLOM), Nvidia Grid K2 (slot2), Magma Expander HBA (slot5), Teradici APEX2800(slot6), Fusion IO drive(slot4)	

Known Behaviors in Release 2.0(7d)

Following are the known behaviors for release 2.0(7d)

Table 84: Cisco IMC

Defect ID	Symptom	Workaround	First Affected Release
CSCuv34476	On the 3260 server, KVM fails to launch and displays the following message: *"Unable to Launch the application"* . This happens after swapping or changing a CMC and making it active or master.	Regenerate the certificate using the Web UI or CLI and reboot the CMC.	2.0(7d)

CSCuv28734	On the 3260 server, boot or crash file download fails with a Network error, when you use the Chrome 43 version browser for downloading.	Use other browsers or use Chrome version 42.	2.0(7d)
CSCuu50850	On the 3260 server, you cannot establish an IPMI session to a BMC when BMC is reset to factory default.	Reconfigure user using active CMC.	2.0(7d)
CSCur77980	On the 3260 server, unable to configure users after resetting CMC to factory defaults. This issue occurs when you attempt to configure a user with a different index number after the reset.	Use the same index number that was used before the reset to configure a user.	2.0(7d)
CSCuu43406	On the 3260 server, the server does not respond and displays an error message when the GUI is idle for a few minutes. This happens when you use Chrome Version 41.	Use other browsers or use Chrome version 42.	2.0(7d)
CSCuu43330	On the 3260 server, unable to login to Web UI when the login screen is left idle for a few minutes. This happens when you use Crome Version 41.	Use other browsers or use Chrome version 42.	2.0(7d)
CSCur60690	On the 3260 server, configuring a user using the CLI or Web UI fails with the following message: **"Error: User with same name <username> already exists."** When a user is configured using the IPMI on BMC the local user, database may not sync with the active CMC. Hence when the same user is configured with a different index on active CMC this error occurs.	Check for the user index number on the local user database on BMC using IPMI and use the same index number to configure the user using the active CMC's CLI or Web UI.	2.0(7d)

Table 85: External Controllers

Defect ID	Symptom	Workaround	First Affected Release
CSCuu36101	On the 3260 server, MegaRAID card does not support raid level migration when the card has maximum allowed number of virtual drives created on it. **Note** Note This is a limitation of the MegaRAID software stack that requires a temporary or ghost VD to do the RLM operation.	Do not create maximum number of allowed virtual drives.	2.0(7d)

Known Behaviors in Release 2.0(6d)

Following are the known behaviors for release 2.0(6d):

Table 86: External Controller

Defect ID	Symptom	Workaround	First Affected Release
CSCui64842	Hardware configuration settings of Broadcom 57810 adapters reset after firmware update. This issue happens on all 57810 adapters. The following settings are reset: • DCB Protocol • SRIOV • Number of VFs per PF	Reconfigure the settings.	1.5(3)

CSCuu35160	While downgrading or upgrading LSI firmware, Cisco IMC log reports several CMD over OOB errors. This is expected behavior and the error messages are due to the controller being briefly unresponsive on out-of-band during firmware update.	None.	2.0(3e)
CSCuu36101	MegaRAID card does not support raid level migration when the card has maximum allowed number of virtual drives created on it. **Note** This is a limitation of the MegaRAID software stack that requires a temporary or ghost VD to do the RLM operation.	Do not create maximum number of allowed virtual drives.	2.0(6d)

Table 87: VIC

Defect ID	Symptom	Workaround	First Affected Release
CSCuu56903	Data traffic between VMs where the vNICs have the same uplink on VIC 1225, could not be switched upstream.	Assign vnic0,vnic1 pinned to Uplink-1 and vnic6,vnic7 to Uplink-2. 1. Note This may affect the physical uplink redundancy.	2.0(3e)

Known Behaviors in Release 2.0(4c)

Following are the known behaviors for release 2.0(4c):

Table 88: Cisco IMC

Defect ID	Symptom	Workaround	First Affected Release

CSCut76388	For the C220 M4 and the C240 M4 servers, power consumption with 1400W PSUs fluctuates when power cap enabled and the power cap value is set towards a lower value within the allowed range.	Set a higher power cap value. For example, if the allowed power cap range is 350W-650W, then set a value higher than 500W.	2.0(4c)
CSCuq39610	The following error appears while configuring SD cards: ERROR_METADATA_EXSISTS	Remove and insert the SD card and re-configure. If the error persist, replace the SD card.	2.0(3d)

Table 89: BIOS

Defect ID	Symptom	Workaround	First Affected Release
CSCur74413	Watchdog timer policy values change while upgrading or downgrading the BIOS firmware between 2.0(3d) and 2.0(3f) versions.	Reset the values after the BIOS firmware upgrade or downgrade.	2.0(3d)
CSCut05524	TxT getting disabled after few reboots.	Use the TPM Clear command in the BIOS to reset the counter and start over again.	2.0(3e)

Table 90: LSI

Defect ID	Symptom	Workaround	First Affected Release
CSCus54600	LSI9271-8i shows Storage Controller Inoperable? fault in UCSM (PMU Fault present in event log)	Replace the LSI9271-8i adapter	2.0(3i)
CSCus68862	Ubuntu (all versions available today) does not have the inbox drivers for any of the IT-based adapters.	None	2.0(3d)

Table 91: VIC

Defect ID	Symptom	Workaround	First Affected Release

CSCut78400	Resetting a VIC adapter to default configuration, using the CLI command adapter-reset-defaults, may result in changing of the default MAC addresses. This may require configuration of the DHCP and OS to correct the changes to the default MAC addresses. The occurs for releases 2.0(4) and later due to moving of the default MAC address range to address certain VIC relates issues.	None.	2.0(4c)

Table 92: External OS

Defect ID	Symptom	Workaround	First Affected Release
CSCuq75761	During installation of Red Hat Enterprise Linux 7, SAN LUNs mapped will not be visible. Server experiences kernel panic, when Red Hat Enterprise Linux 7 OS is installed on local storage and a SAN LUN is mapped.	No workaround. A driver update disk may be available later to address this issue.	2.0(2c)

Table 93: External Controllers

Defect ID	Symptom	Workaround	First Affected Release
CSCuq43129	OL 5.9 and OL 5.10 operating systems do not recognize QLE2672 SAN LUN during installation.	None.	2.0(3d)

CSCuq60947	Citrix XenCenter 6.2 configured VM instances fails to boot when driver is passed and vGPU is disassociated.	Perform the following steps to disassociate vGPU from VM instance: **1.** From the VM console, choose Start > Control Panel > Hardware and Sound > Device Manager > Display Adapters > Nvidia K1 or K2. **2.** Right click and choose **Uninstall** . **3.** Power off the VM from XenCenter console. **4.** In th eXenCenter console, open VM Properties. **5.** Right click the GPU in left column and choose GPU type: > None. **6.** Boot up the VM.	2.0(3d)

Known Behaviors in Release 2.0(3d)

Following are the known behaviors for release 2.0(3d):

Table 94: BIOS

Defect ID	Symptom	Workaround	First Affected Release

CSCuq99268	For the ESXi 5.5 and later updates, you can install the OS on a disk behind Cisco 9300 HBA using the native inbox driver (lsi-msgpt3). However, lsi_msgpt3 is not fully supported. Therefore it must be disabled and the async drivers must be installed.		2.0(3d)

		After installing the OS, complete the following steps to install the mpt3sas drivers: 1. **#esxcli software vib install -v file:/{FULL_PATH_TO_YOUR_VIB(..xxx.vib)}** 2. Disable lsi-msgpt3 (native driver) using the following command: #esxcfg-module ?d lsi-msgpt3 3. If the system is restarted, as a rule, the mpt3sas driver should take over. Verify this using the following command: ~ **# esxcli storage core adapter list:** `HBA Name Driver Link State UID Description -------- ------- ----------- ---------- ---------- vmhba0 ahci link-n/a sata.vmhba0 Intel Corporation Patsburg 6 Port SATA AHCI .. vmhba1 mpt3sas link-n/a sas.xxxxxxx LSI / Symbios Logic SAS3008 PCI-Express .. vmhba32 ahci link-n/a sata.vmhba32 Intel Corporation Patsburg 6 Port SATA AHCI .. vmhba33 ahci link-n/a sata.vmhba33 Intel Corporation Patsburg 6 Port SATA AHCI .. vmhba34 ahci link-n/a sata.vmhba34 Intel Corporation Patsburg 6 Port SATA AHCI .. vmhba35 ahci link-n/a sata.vmhba35 Intel Corporation Patsburg 6 Port SATA AHCI .. vmhba36 ahci link-n/a sata.vmhba36 Intel Corporation Patsburg 6 Port SATA AHCI ..` 4. If the driver name is still listed as lsi-msgpt3 for the above command, try removing (instead of disabling) lsi-msgpt3 using the following command: #esxcli software vib remove ?n lsi-msgpt3	

		5. Restart the system.	
CSCup89033	The Power Monitoring graph is displayed on top of all pages if the Power Monitoring page is loading and you navigate to any other page.	Navigate back to the Power Monitoring page and wait till the page loads and then navigate to any other page.	2.0(3d)
CSCuq00837	On C220 M4 and C240 M4 servers, TPM fails to initialize after installing ESXi 5.1 U2 Patch 05, and enabling and activating TPM and TXT.	No workaround.	2.0(3d)
CSCuq04009	ESXi installer does not detect any SD card in xHCI mode.	Disable USB xHCI mode in the BIOS.	2.0(3d)
CSCuo28585	HII Drive Management and Enclosure Management menu displays only one port/connection (0-3) and not the other (4-7) when an expander is connected to a controller through two ports.	No workaround.	2.0(3d)
CSCuq14862	With inbox IGB driver in SLES 11 SP3, ethtool shows incorrect firmware version for Intel i350 LOM after installing the drivers for Intel i350 LOM from 2.0(3d) drivers ISO(5.2.5).	Update the igb version to 5.2.5. Unload and load the igb.	2.0(3d)
CSCuq24196	After installing the Windows Server 2012 to an iSCSI LUN, few network adapters display a yellow bang in the device manager (code 10) with the following description: This device is not working properly because Windows cannot load the drivers required for this device This occurs only on the NICs that are used for iSCSI boot.	Perform one of the following: A hotfix is available for Windows 8 and Windows Server 2012. Run this fix in the Windows OS image and then perform iSCSI installs. For more information on the fix, see http://support.microsoft.com/kb/2822241 OR Complete the following steps : 1. Un-install the drivers for the device which is showing yellow bang without deleting the device. 2. Re-install the drivers. 3. Restart the server.	2.0(3d)

CSCup82749	Windows 2K12 R2 iSCSI Boot with Intel i350 and Pinecrest adapters displays BSOD when it is installed using the inbox drivers.	While installing the W2K12 R2 iSCSI, skip the Intel drivers from the drivers ISO. Reboot the server once the installation is finished.	2.0(3d)
CSCuq92331	Bandwidth test fails while running synthetic benchmarks, like the nvqual. This happens when the processor power management is enabled.	Disable the processor power management option using the BIOS setup.	2.0(3e)
CSCuo05774	Setting the boot mode to UEFI or Legacy requires two reboots for the change to reflect.	Reboot the server twice.	2.0(3e)
CSCul04884	Server enters BIOS setup menu when the boot devices that are configured in the service profile are not found. This impacts only C-series servers that are managed by Cisco UCS Manager.	None.	2.0(3e)
CSCuj28644	UEFI PXE boot or UEFI iSCSI boot does not work when the boot mode is set to UEFI.	Use the legacy boot mode when using PXE or iSCSI boot.	2.0(3e)

Table 95: Cisco IMC

Defect ID	Symptom	Workaround	First Affected Release
CSCuo26946	When you upgrade from releases 1.5(x) to 2.0(x) or downgrade from 2.0(x) to 1.5(x) or migrate from legacy to precision boot order, and if the SD card has four partitions, BIOS boot order mismatch occurs for the SD cards.	No workaround. You have to re-configure the boot order.	2.0(3d)
CSCuq32910	When the server boots with 2.0.3d release firmware, it fails to update the HUU firmware version and displays the current version of the Emulex OCe14102/Oce11102 as **Not** .	Reboot the server.	2.0(3d)

Table 96: External Controller

Defect ID	Symptom	Workaround	First Affected Release
CSCup87719	i350 adapter with default factory configuration dispatches the boot protocol Option ROM only for the first port. It does not dispatch Option ROM for the remaining 3 ports of the i350 card.	Enable the boot option for required ports using boot Util.	2.0(3d)

Known Behaviors in Release 2.0(1b)

Following are the known behaviors for Release 2.0(1b):

Table 97: Cisco IMC

Defect ID	Symptom	Workaround	First Affected Release

CSCup49368	When you click **Update All** to upgrade from version 1.5.7 to 2.x using the **Cisco Host Upgrade Utility** the chassis firmware does not get updated.	Using the Web UI, complete these steps to upgrade the chassis firmware: **1.** In the **Navigation** pane, click the **Server** tab. **2.** On the **Server** tab, click **Summary**. **3.** In the **Actions** area, click **Power Off Server**. **4.** Click **OK** to power off the server and updates the system firmware. Using the CLI, complete these steps to upgrade the chassis firmware: **1.** Server# **scope chassis** **2.** Server /chassis # **scope firmware** **3.** Server /chassis/firmware # **show detail**: `Firmware update required on some components, please run update-all (under chassis/firmware scope).` **4.** Server /chassis/firmware # **update-all**	2.0(1b)
CSCup58906	When you downgrade to 2.0(1a), Cisco IMC Web UI displays warning messages and critical events.	A/C Power cycle the sever.	2.0(1b)

Known Behaviors in Release 2.0(1)

Following are the known behaviors for the Release 2.0(1):

Table 98: Cisco IMC

Defect ID	Symptom	Workaround	First Affected Release
CSCth84883	The LED sensor color is red or amber or blue (or any supported color) even though the LED state is set to OFF.	Ignore the LED color when the LED state is set to OFF.	2.0(1)
CSCtt08424	Cisco IMC power capping is not supported on VMware ESXi 5.0.	When Cisco IMC is upgraded to 1.4(2), the Cisco IMC will automatically disable power capping. Power capping must manually be re-enabled to use it.	2.0(1)
CSCun97225	When you downgrade from release 2.0(1a) to a 1.5(x) release, you see only seven platform event filters instead of 12 filters.	Restore factory default settings or run the Cisco OEM function command on the ipmitool raw **0x36 0x03 0xAA** .	2.0(1)
CSCuo40835	When you downgrade from release 2.0(1a) to a 1.5(x) release, if you have set the SNMP port value to anything other than the default value (161), you cannot reset this number.	Before downgrading, set the SNMP port to 161 or after downgrading restore factory defaults.	2.0(1)
CSCun10320	Cannot upgrade Cisco IMC firmware version from 1.5(3d) to 2.0(1a) using FTP.	Use a browser or SCP client upgrade.	2.0(1)
CSCum70086	Downloaded DVR player fails to play offline for Java versions 6 and below on Windows OS.	Edit and update the **script_win.bat** file with the correct Java version.	2.0(1)
CSCun66062	While using the CLI to define the precision boot order, if multiple devices' orders are changed by scoping to an individual device, the final order of the devices may not appear as what it was changed to.	Use the **rearrange-boot-device** command to set the boot order for multiple devices. Or use the Cisco IMC Web UI.	2.0(1)

CSCum26002	A delay occurs while pinging to check the connectivity to the DNS servers before a DDNS update is triggered.	You can manually check the connectivity to the preferred and alternate DNS servers for both the IPv4 and IPv6 addresses the using the ping option available in this release.	2.0(1)
CSCun11979	Cannot configure legacy boot order using the Cisco IMC Web UI.	Use CLI or XML API.	2.0(1)
CSCuo71634	After upgrading the Cisco IMC firmware and activating secure boot mode, when you immediately try to reboot Cisco IMC, it does not respond.	After the upgrade, reboot Cisco IMC after about 10 minutes.	2.0(1)

Known Behaviors in Release 1.5.7

Following are the known behaviors for Release 1.5(7):

Table 99: CIMC

Defect ID	Symptom	Workaround	First Affected Release
CSCul62033	During heavy I/O transactions on the SD card, read errors may be seen in CIMC.	Use Cisco FlexFlash 3.0 cards	1.5(7)
CSCua94308	There is no CIMC notification of Closed Loop Thermal Throttling (CLTT) when it occurs. CLTT happens automatically when the DIMM temperature crosses the UC (upper critical) temperature.	None.	1.5(7)
CSCuo18891	UCScfg_X64.exe batch -ignore set t.txt command displays "Error: Invalid Number of Arguments" error message, when the input file is in Unicode format.	Use ANSI format input file. (	1.5(7)

CSCud84978	SEL has memory entries, but no entries are seen in the fault page. Cisco UCSM fault codes are unavailable for these SEL.	None. SEL has to be used to decode the memory related events.	1.5(1)

Table 100: OS

Defect ID	Symptom	Workaround	First Affected Release

CSCun77988	After installation of ESXi in UEFI mode, the OS fails to boot up. The installation completes, but on the subsequent reboot, the server does not boot ESXi OS.		1.5(7)

			To resolve this issue, complete these steps: **1.** Boot to Shell. **2.** Determine fsxx (xx is where ESX is installed. It will be typically 0 i.e fs0:) This can be verified by using fsxx\EFI\Boot\BOOTX64.EFI command. **3.** To get the current list of EFI Boot options use, **bcfg boot dump** command. **Note** Save the last boot number for further use. **4.** Use the following command to add new Boot Option at position LAST_BOOT_NO + 1. Last parameter in quotes can be any description for this new Boot Option. This is displayed during BIOS F6 menu - **bcfg boot add LAST_BOOT_NO + 1 fsxx\EFI\BOOT\BOOTX64.EFI "UEFI: ESXi"** **5.** Make the newly created Boot Option for ESX as the first by using **bcfg boot mv LAST_BOOT_NO + 4 1** command. Reset the platform by issuing reset command at the shell. Press F6 when BIOS is booting to get	

		into BIOS Boot Selection menu. Verify that newly created Boot Option is displayed. Select this and boot to ESX.	

Table 101: NVIDIA

Defect ID	Symptom	Workaround	First Affected Release
CSCuo39368	Nvidia GPU cards non functional or erratic behavior on system beyond 1 TB of memory.	This is an Nvidia GPU limiation due to 40 bit addressing on the GPU's. The memory should be 1 TB or less for the GPU's to be functional.	1.5(7)

Table 102: LSI

Defect ID	Symptom	Workaround	First Affected Release
CSCue88244	Prepare for removal prepares a Hard drive for removal but LED on the HDD does not blink AMBER to indicate the drive is ready to be replaced. This happens only on direct connect C260 M3 configurations.	None.	1.5(4)

CSCui29979	BBU Charging Status shows either Charging or Discharging all the time. This could lead to confusion to customers as Charging or Discharging indicate that battery is not in optimal state.	Customers should use the BBU Status field to determine if the battery is in optimal state. If the BBU status is optimal, it will indicate a good battery. If the BBU status indicates battery needs replacement, then the BBU is bad and needs to be replaced. Charging Status is working as designed and will always indicate Charging or Discharging because Firmware keeps checking the battery charge and ensures that the charge does not fall below the band gap. It charges the battery when it is in lower limits and once it reaches the upper limit of the band, it will stop charging. There can be leakage current which can discharge the battery and bring it back to lower threshold. When this happens, the firmware initiates charging.	1.5(2)

Known Behaviors in Release 1.5(4)

Following are the known behaviors for Release 1.5(4):

Table 103: BIOS

Defect ID	Symptom	Workaround	First Affected Release
CSCul36732	SAN boot using Emulex adapters may fail on C-series servers managed by Cisco UCS Manager. This behavior occurs only on servers managed by Cisco UCS Manager.	During the BIOS post, press the hotkey to enter the Emulex Option ROM configuration screen and enable "EDD", save and exit.	1.5(4)
CSCub21433	UEFI OS install is not supported on Software RAID (Onboard SCU controller).	None. Use legacy mode OS installs when using Software RAID.	1.5(4)

CSCtz11862	Continuous beep sound is heard when the system is switched on.	Do not switch on the CIMC and the host simultaneously. Switch on the host 3 minutes after switching on the power supply.	1.5(4)

Table 104: CIMC

Defect ID	Symptom	Workaround	First Affected Release
CSCuj89681	After moving an SD card to the single partition mode, if you downgrade to releases prior to 1.5(4x), all 4 partitions are visible in the WebUI/CLI.	None.	1.5(4)
CSCuj84718	SD card partition sizes appear as trash values for SCU,HUU and drivers during downgrade.	Upgrade to release 1.5(4x) and create a single partition, and then downgrade to a prior release. The partition sizes then appear to be 2097151 MB.	1.5(4)
CSCuj67995	Changing multiple configuration with Port parameter fails from CIMC configuration only.	Complete the following steps: **1.** Set the mode to **Dedicated** and the redundancy to **None**. **2.** Save the changes to the system. **3.** Set the auto-negotiation field to **Yes**.	1.5(4)
CSCuj52943	In the transition from 4 partition configuration to a single partition, only configuration details are modified. Data on the SD remains intact. So after migrating to a single partition (HV), the HV partition will retain SCU data only if SCU has a valid file system during configuration migration.	After migrating to a single partition (HV) configuration, format and install the required OS on the HV partition.	1.5(4)

CSCul50285	ucs-c220-m3# scope bios/advanced ucs-c220-m3 /bios/advanced # ucs-c220-m3 /bios/advanced # set ConsoleRedir COM_0 ucs-c220-m3 /bios/advanced *# set BaudRate 115200 ucs-c220-m3 /bios/advanced *# set FlowCtrl None ucs-c220-m3 /bios/advanced *# set TerminalType VT100+ ucs-c220-m3 /bios/advanced *# commit ucs-c220-m3 /bios/advanced #	Use the following process: ucs-c220-m3# scope bios ucs-c220-m3 /bios #scope advanced ucs-c220-m3 /bios/advanced # set ConsoleRedir COM_0 ucs-c220-m3 /bios/advanced # commit Changes to BIOS set-up parameters will require a reboot. Do you want to reboot the system?[y|N]	1.5(4)
CSCue10121	The PWRGD Sensor's Normal events are logged in the SEL during the CIMC boot and Host boot.	These are expected events and can be ignored.	1.5(4)
CSCuj41445	Auto complete for few fields is done.	Upgrade to 1.5(x) build.	1.5(4)
CSCud17092	Occasionally after a CIMC upgrade, one may see an error dialog box "Error: Unexpected error" in Web UI on main page upon the very first login. The Storage data may also be blank or invalid. Sometimes occurs during the very first login after a CIMC upgrade. It may be related to upgrade from 1.4x to 1.5.	Logging out and back in will fix it, but probably just because it takes time; therefore, just waiting a few minutes and refreshing the WebUI may fix the problem, also.	1.5(4)

Table 105: Cisco usNIC

Defect ID	Symptom	Workaround	First Affected Release
CSCul56178	CIMC limits the configurable vNICs, and usNICs to 229.	None. The remaining vNICs are reserved for the internal adapter usage. Of these remaining vNICs, 4 are mandatory- 2 eNICss, and 2 fNICs. When you configure 16 vNICs (including the 2 mandatory eNICs), you are left with 229-2(fNICs)-16(eNICs)= 211 usNICs.	1.5(4)

Table 106: LSI

Defect ID	Symptom	Workaround	First Affected Release
CSCuj83316	The battery is in a degraded state because it requires a manual (user initiated) relearn cycle.This is required of batteries that have been in use for over 1 year to accurately measure the battery's remaining capacity.	A manual (deep cycle) relearn must be started by the user. This can be done via the MegaCLI utility or from the Storage tab of the server CIMC. A relearn can take several hours and up to a day to complete. It the battery still has sufficient capacity after the relearn is complete, it will go to optimal state and the VDs will switch back to WriteBack mode if that is how they configured prior to the relearn.	1.5(4)

Table 107: Web Management

Defect ID	Symptom	Workaround	First Affected Release

CSCtx16030	The WebUI DIMM "Operability" field in the memory inventory does not indicate failed DIMMs correctly.	The issue is observed only in the memory inventory reported by the WebUI. The BIOS reports the DIMM status properly in the BIOS Setup. So, if WebUI shows any DIMM as Inoperable, please check the status of all DIMMs on all the memory risers at Advanced -> Memory Configuration page of the BIOS Setup to get the correct status on the DIMMs.	1.5(4)

Known Behavior in Release 1.5(3)

Following are the known behaviors for Release 1.5(3):

Table 108: Firmware Upgrade

Defect ID	Symptom	Workaround	First Affected Release
CSCui82263	Downgrading from release version 1.5(3) to 1.5(1) release version does not throw an error in Host Upgrade Utility.	This is not an issue. Though an error is not reported, the update will not proceed.	1.5(3)

Known Behaviors in Release 1.5(2)

Following are the known behaviors for Release 1.5(2):

Table 109: CIMC

Defect ID	Symptom	Workaround	First Affected Release
CSCuf52723	C240 M3 does not power up after firmware upgrade to 1.5(1B). While upgrading via HUU from firmware 1.4(6c) to 1.5(1b), HUU did not upgrade CIMC to 1.5(1b) even though it reported as successfully completed.	Manually force CIMC and BIOS update to fix it.	1.5(2)

CSCug78887	Base Distinguished Name (base-dn) parameter syntax is different in new LDAP implementation.	Use the following syntax:
		`/ldap # set base-dn DC=Scom,DC=msdn,DC=com`
		instead of
		`/ldap # set base-dn Scom.msdn.com`
			1.5(2)

CSCuh71550	With Windows Active Directory, the child domain user login will fail with partial login name.	Provide fully qualified login name to make it work.	1.5(2)
CSCuh39061	Intel VTD and ATS are required BIOS setting for usNIC. However, there is no warning message in CIMC if these parameters are not enabled when usNIC is configured.	Make sure Intel VTD and ATS are enabled in BIOS setting when usNIC is configured.	1.5(2)
CSCuf08450	When upgrading the C24 M3 from 1.4.7a to 1.4.7f using the HUU (option to upgrade all), the servers fans run at almost double the speed they were running at on 1.4.7a.	None	1.5(2)
CSCug65160	Sometimes, a VIC link on a SFP+ copper cable goes down after a VIC reboot or CIMC reboot. Cables whose serial number starts with MOC1238 through MOC1309 could be affected.	AC power cycle the chassis to recover.	1.5(2)
CSCtx43305	The PSU firmware revision may only be partially available when the PSU does not have AC power.	Connect the AC power to the PSU. The full firmware revision will be available.	1.5(2)

Table 110: LSI

Defect ID	Symptom	Workaround	First Affected Release

CSCue10144	When booting a Cisco C22x or C24x server, RAID levels are displayed when loading the LSI Option ROM. However, not all supported RAID levels are displayed.	This is done to distinguish between different 9240 controllers. Some of them support RAID5, and some do not. There are 2 products under the same 9240 name. However, there is not enough space in the name field to list every possible RAID level supported. This is why a partial list of RAID levels is displayed.	1.5(2)
CSCug95648	BBU charging status always shows as Charging and percentage of charging never reaches to 100%. It always shows 67%.	This is the new change in the firmware. The Battery re-learn cycle is completed successfully and battery is charged back to 67% which is in the band gap where charging will be stopped by LSI firmware and battery will be declared optimal. This is the charge needed to retain data upto 48 hours. The Charging Status showing "Charging" as there will be some leakages and battery will slowly loose charge and hence the battery will be charging.	1.5(2)
CSCuh82265	BBU status is showing as discharging and the charge % is stuck at 64%. Battery replacement alerts on the server. Server is showing battery discharging and there is a moderate alert which says Status: Learning Cycle Needed?	None	1.5(2)
CSCud13257	Hang occurs when using 64-bit MSM 12.08.03.03.	Use 32 bit version of MSM.	1.5(2)

Table 111: Host Upgrade Utility

Defect ID	Symptom	Workaround	First Affected Release

CSCui09482	Firmware Update on Emulex LPe16002 will fail when tried from HUU on certain servers.	Emulex LPe16002 is already at the same firmware level of what HUU is carrying. So effectively an update is not needed. alternatively move the card to another server and try update.	1.5(2)

Table 112: SNMP

Defect ID	Symptom	Workaround	First Affected Release

CSCug37639		None.	1.5(2)

When doing a MIB walk on several MIBs, they give a "No more variables left in this MIB View (It is past the end of the MIB tree)" error at the end. Failing MIBs: snmpVacmMIB

Sample good output:

```
[root@pebbles-iptv mibs]#
snmpwalk -v2c -c public
localhost
notificationLogMIB
NOTIFICATION-LOG-
MIB::nlmConfigGlobalAgeOut.0
= Gauge32: 1440 minutes
NOTIFICATION-LOG-
MIB::nlmStatsGlobalNotificationsLogged.0
= Counter32: 33
notifications
NOTIFICATION-LOG-
MIB::nlmStatsGlobalNotificationsBumped.0
= Counter32: 33
notifications
[root@pebbles-iptv mibs]#
**
```

Notice MIB ends cleanly, and there is no error.

** Sample bad output:

```
[snmp@sv-repo ~]$ snmpwalk
-t 120 -v3 -u glasco -l
AuthPriv -a MD5 -A
enuf4me2do -x DES -X
tqbFjotlCow 14.17.2.45
.1.3.6.1.6.3.16.1.5.2.1.6
SNMP-VIEW-BASED-ACM-MIB::vacmViewTreeFamilyStatus."all".1.1
= INTEGER: active(1)
SNMP-VIEW-BASED-
ACM-MIB::vacmViewTreeFamilyStatus."_all_".1.0
= INTEGER: active(1)
SNMP-VIEW-BASED-ACM-
MIB::vacmViewTreeFamilyStatus."_all_".1.1
= INTEGER: active(1)
SNMP-VIEW-BASED-ACM-
MIB::vacmViewTreeFamilyStatus."_all_".1.2
= INTEGER: active(1)
SNMP-VIEW-BASED-ACM-
MIB::vacmViewTreeFamilyStatus."_none_".1.0
= INTEGER: active(1)
SNMP-VIEW-BASED-ACM-
```

	MIB::vacmViewTreeFamilyStatus."_none_".1.1 = INTEGER: active(1) SNMP-VIEW-BASED-ACM- MIB::vacmViewTreeFamilyStatus."_none_".1.2 = INTEGER: active(1) SNMP-VIEW-BASED-ACM- MIB::vacmViewTreeFamilyStatus."_none_".1.2 = No more variables left in this MIB View (It is past the end of the MIB tree) [snmp@sv-repo ~]$ To have, "No more variables left in this MIB View" when there are more mibs left to walk. The final oid seen is 1.3.6.1.6.3.16.1.5.2.1.6, and within the error-status of the get-response packet, we get noSuchName(2), and this should be noError(0).		

Table 113: Web Management

Defect ID	Symptom	Workaround	First Affected Release
CSCuc19323	Sometime with Windows 2008 and IE 8.0 CIMC WEB UI login prompt will not be seen	Add CIMC IP to IE 8.0 trusted sites list. In the Internet Explorer browser window, select Tools -> Internet options -> Security -> Trusted Sites -> Sites -> Add	1.4(7)
CSCuh76949	After clicking on "Add Exception", user is prompted with a window which says "certificate is valid" and the "Confirm Security Exception" button is greyed out.	Clear the cache or refresh multiple times the issue will be resolved.	1.5(2)

Known Behaviors in Release 1.5(1f)

Following are the known behaviors for Release 1.5(1f):

Table 114: CIMC

Defect ID	Symptom	Workaround	First Affected Release

CSCuf53059	FlexFlash operational profile is not preserved on downgrade from 1.5(1x), resulting in all FlexFlash partitions being visible to the operating system.	Set the operational profile again after downgrade.	1.5(1f)

Table 115: Intel RSTe

Defect ID	Symptom	Workaround	First Affected Release
CSCuf02487	Creating RAID volumes from Intel RSTe software RAID Option ROM (Control-I) is not supported.	Use LSI software RAID, LSI hardware RAID, or OS SW RAID.	1.5(1f)
CSCue72256	Hard drive Critical events are seen in SEL during server bootup when using Intel RSTe.	This is not a real hard drive fault. The HDD Critical events reported becomes normal after system boots up and can be ignored. If real HDD fault, then Critical event generated on HDD will be persistent and does not indicate normal even after server has booted up and in this case, user need to take action to replace that HDD.	1.5(1f)

Known Behaviors in Release 1.5(1)

Following are the known behaviors for Release 1.5(1):

Table 116: BIOS

Defect ID	Symptom	Workaround	First Affected Release
CSCuc75369	LSI Web BIOS may not launch on pressing Ctrl+H.	During BIOS post, press F6 to bringup the boot override list and select the appropriate entry to launch the web bios.	1.5(1)
CSCuc60934	BIOS Boot order is getting changed when a virtual media device is mounted and unmounted through CIMC WebUI vKVM console or CIMC CLI.	After unmounting the virtual media device, restore the boot order by re-configuring the boot order through either BIOS Setup or CIMC.	1.5(1)

CSCtf54851	Serial port B cannot be enabled for console redirection in the Server Management -> Console Redirection page of the BIOS setup.	Serial port B is primarily used for SOL functionality. The BIOS will start redirecting console messages to serial port B if SOL is enabled. You should enable SOL through BMC to get console redirection messages through serial port B.	1.5(1)
CSCth71350	If the current CIMC networking mode is shipping mode, then the BIOS F8 CIMC configuration utility does not allow a new networking mode and IP address to be set at the same time.	Set the new networking mode, save, then set the new IP address and save again.	1.5(1)
CSCtq84425	When BIOS console redirection is enabled, the keyboard can stop working in the Broadcom PCIe Option ROM at some baud rates.	Disable the BIOS console redirection.	1.5(1)
CSCtx27907	Occasionally, when BIOS starts, the following message is displayed: Error on Getting Cisco IMC IP/MAC Address.	This message can be ignored.	1.5(1)
CSCtx92042	When Broadcom 5709 Gigabit Ethernet adapter is plugged into one of the PCIE slots, the server gets stuck at the BIOS post screen during the booting process.	Upgrade the firmware on the Broadcom 5709 Gigabit Ethernet adapter to version 5.2.7 or later.	1.5(1)
CSCtr93601	BIOS downgrade using the iFlash32 utility, from 1.4.x to the older version 1.2.x fails.	Use the startup.nsh script available in the 1.2.x container for the downgrade. This script will execute the BIOS downgrade successfully.	1.5(1)

Table 117: CIMC

Defect ID	Symptom	Workaround	First Affected Release

CSCuf05110	CIMC CLI does not report PID of HDD when using Intel RSTe.	None	1.5(1)
CSCue54670	For a server with Virident card (or any card for which fan control has specific modifications), if CIMC is reset to factory defaults when host is on, then the fan control will go back non-card specific settings. This might imply lower fan speeds and can cause heating up of cards if there are cards present that require higher fan speeds (ex: Virident FlashMaxII card). This is because information about cards is available to CIMC from host, and when a factory default is done, this information is erased.	Reboot the host, so that CIMC can get card specific information and bump up fan speeds as required.	1.5(1)
CSCtg92856	When you power on the chassis with some PS power cables disconnected, the system health LED on the front panel stays green, though some power supplies have no input voltage.	Connect all cables from APC power to the power supply securely.	1.5(1)

CSCtz52715	USB Key which is inserted on a Mac can be forced to be read-only.	Mac users must unmount the removable drive before mapping. 1. Run the following command from the command line interface: `diskutil unmount /Volumes/<Volume name>` 2. In the KVM/vMedia client, clear the Read Only checkbox. At this point, the user may be prompted asking if they wish to stop automatic mounting of the drive. Click Yes . 3. Proceed with mapping the drive. These steps are time-sensitive, as the Mac OS is aggressive about re-mounting drives that have been unmounted. If the drive does get re-mounted by the OS before completing the steps, repeat the steps. Alternatively, unmap the USB stick, use the Finder to eject the device, wait for the device to disappear from the vMedia Client view, and then physically remove and re-insert it while the vMedia session is running. As above, click Yes to the questions asking about preventing automatic mounting of the drive.	1.5(1)

CSCua63839	On some Macs with spaces enabled, the vKVM popup notification that the session has ended can not be closed because trying to click the button causes the focus to move away from the space with the popup.	Move the vKVM main window to the same space with the popup notifier. Then, the popup can be dismissed by clicking on the button.	1.5(1)
CSCtr37876	SNMPv1 traps are sent when SNMPv2 and SNMPv3 traps are enabled.	None.	1.5(1)

CSCtx00839	The KVM screen displays a blank screen.	Use the physical monitor to change the screen resolution. The following resolutions are supported: • 640x480 (8bpp) • 800x600 (8bpp) • 1024x768 (8bpp) • 1280x1024 (8bpp) • 1600x1200 (8bpp) • 1920x1080 (8bpp) • 1920x1200 (8bpp) • 640x480 (16bpp) • 800x600 (16bpp) • 1024x768 (16bpp) • 1280x1024 (16bpp) • 1600x1200 (16bpp) • 1920x1080 (16bpp) • 1920x1200 (16bpp) • 640x480 (24bpp) • 800x600 (24bpp) • 1024x768 (24bpp) • 1280x1024 (24bpp) • 640x480 (32bpp) • 800x600 (32bpp) • 1024x768 (32bpp) • 1280x1024 (32bpp)	1.5(1)

CSCtx88183	After firmware updates, the CIMC Web GUI and CLI might not display the Virtual Drive Information under the Virtual Drive tab and might display the Virtual Drive count as zero even though the Virtual Drive tab displays the list of virtual drives present in the system.	Restart the Cisco IMC.	1.5(1)
CSCty58229	The SNMP Hard Disk Inventory starts numbering with 0 while the CIMC HDD sensor starts with 1.	None. This symptom occurs because the SNMP Hard disk inventory matches with the storage inventory and both starts with index 0. The hard disk sensor numbering starts with 1 because it matches with the label in the SKU. You need to be aware of the difference and map it accordingly while browsing for a specific HDD detail across sensors and storage inventory.	1.5(1)
CSCty60975	The HDD presence cannot be viewed through SNMP.	Use either alternate interfaces or do SNMP query again for the HDD inventory after the action.	1.5(1)
CSCua11831	Duplicate SNMP traps are obtained when you insert Fan 2,4 and 5 in Cisco C22.	None.	1.5(1)
CSCuc87936	"Unable to communicate with FlexFlash" error message is seen after downgrading CIMC to version 1.4.	User should select the Reset Flex Controller button twice if the SD card is of type SD253. If not, select the button only once.	1.5(1)

Table 118: Intel Adapters

Defect ID	Symptom	Workaround	First Affected Release

CSCuc52172	When multiple Intel network adapters are present and you enter the iSCSI configuration from one card, it allows you to change the configuration on all Intel cards. After the change, when one of the cards is removed, it appears that the Option ROM of the remaining cards is overwritten by the card that was removed.	Enter the iSCSI configuration of the card that must be modified. Do not modify other cards when they are visible. This issue is only with iSCSI configuration and not with PXE configuration.	1.5(1)

Table 119: LSI

Defect ID	Symptom	Workaround	First Affected Release
CSCtg25373	If the number of Virtual Drives created in the LSI MegaRAID controller is greater than or equal to 50, the system will not boot from any of these Virtual Drives.	None. The system boots from MegaRAID Virtual Drives only if the number of Virtual Drives are lesser than or equal to 49.	1.5(1)
CSCua03604	RHEL 6.2 Install to iSCSI target hangs when 2008 MEZZ card Option ROM is disabled on C220/C240 M3 servers.	2008 LSI OPROM must always be enabled in System BIOS when it is present in the server. If users want to disable it, then during OS Installs, depending on the OS, they would need to blacklist the LSI MegaRAID driver for the 2008 MEZZ card so that system will not hang during install.	1.5(1)

CSCts37240	The following error message is displayed in some LSI RAID controllers when you navigate to Cisco IMC > Inventory > Storage > Battery Backup Unit . Error: required HW is missing (i.e Alarm or BBU) The server did not have BBU installed on it and it should have confirmed the absence of the unit.	None. This issue is currently under investigation.	1.5(1)

Table 120: Web UI

Defect ID	Symptom	Workaround	First Affected Release
CSCtc22985	Printing from Web UI is not supported.	Print a screenshot of Web UI.	1.5(1)

Known Behavior in Release 1.4(3)

Following is the known behavior for Release 1.4(3):

Table 121: CIMC

Defect ID	Symptom	Workaround	First Affected Release
CSCun24570	Unable to set all numeric CN from the WebUI.	Update the CN from CLI	1.4(3)

Recommended Best Practices

Best Practices to Install VMWare

Workaround for Installing VMWare on First Generation (Gen 1) SD Cards in Expert Mode

Once you start the installer application, find the partition where you want to install VMWare. In the following example the partition is **vmhba33:C0:T0:L0.**

1. Press Alt+F1 to enter the VMWare recovery console.
2. Create a GUID Partition Table (GPT) on the disk:

   /dev/disks # partedUtil mklabel mpx.vmhba33:C0:T0:L0 gpt
3. Verify the GPT:

   /dev/disks # partedUtil get mpx.vmhba33:C0:T0:L0

   3785 255 63 60817408
4. Return to installing VMWare.

Upgrading BIOS and Cisco IMC Firmware

Cisco provides the Cisco Host Upgrade Utility to assist you in upgrading the BIOS, Cisco IMC, CMC LOM, LSI storage controller, and Cisco UCS Virtual Interface Cards firmware to compatible levels. On the C220 M3, C240 M3, C22 M3, and C24 M3 servers, we recommend that you reboot Cisco IMC before performing the Cisco IMC and BIOS firmware update using NIHUU, HUU, web UI, CLI, or XML API.

Note When upgrading the Cisco IMC firmware for the UCS C-series platforms, ensure that you update using the full image (for example upd-pkg-cXXX-mx-Cisco IMC.full.*.bin).

The correct and compatible firmware levels for your server model are embedded in the utility ISO.

To use this utility, use the Cisco Host Upgrade Utility User Guide which includes the instructions for downloading and using the utility ISO. Select the guide from this URL:

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

Related Documentation

Related Documentation

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

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

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

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

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

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

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

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