Release Notes for Cisco UCS C-Series Software, Release 3.0(2)

First Published: 2017-01-13

Cisco UCS C-Series Servers

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

About the Release Notes

This document describes the new features, system requirements, open caveats and known behaviors for C-Series software release 3.0(2) including Cisco Integrated Management Controller software and any related BIOS, firmware, or drivers. Use this document in conjunction with the documents listed in the Related Documentation section.

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

Revision History

Revision	Date	Description
A0	January 13, 2017	Created release notes for Release 3.0(2).

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.

Overview of the Server Models

Overview of Servers Supported for Release 3.0(2)

The following servers are supported in this release:

- UCS-C240 M4
- UCS-C220 M4

For more information, see Overview of Servers

Hardware and Software Interoperability

For detailed information about storage switch, operating system, adapter, adapter utility, and storage array interoperability, 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

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

Cisco UCS C-Series and Cisco UCS Manager Release Compatibility Matrix for C-Series Rack-Mount Servers

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

The following table lists the C-Series software standalone and Cisco UCS Manager releases for C-Series Rack-Mount Servers:

Table 1: Cisco C-Series and UCS Manager Software Releases for C-Series Servers

C-Series Standalone Release	Cisco UCS Manager Release	C-Series Servers
3.0(2b)	No Support **Note** We support discovery and upgrade or downgrade functions with Cisco UCS Manager.	C220 M4/C240 M4 only
3.0(1d)	No Support **Note** We support discovery and upgrade or downgrade functions with Cisco UCS Manager.	All M3/M4 except C420 M3
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
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

C-Series Standalone Release	Cisco UCS Manager Release	C-Series Servers
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

Upgrade Paths for Release 3.0(x)

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

Table 2: Upgrade Paths to Release 3.0(x)

Upgrade From Release	Upgrade To Release	Recommended Upgrade Path
Incase of C460 M4 for release lesser than 2.0(4c)	3.0(x)	Follow these steps to upgrade from releases less than 2.0(4c) to 3.0(x): **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(x)** • 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(x)	3.0(x)	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(x)	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(x) and releases lesser than 1.5(4)	3.0(x)	**Before update, Reboot the bmc.** **Upgrade from 1.4(x) to 1.5(4)** • Use Interactive HUU, Non-Interactive HUU (NIHUU) script not supported for 1.4(x) • 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(x)** • 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(x)	**Upgrade from 1.5(x) 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(x)** • 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.

Transceivers Specifications

The Cisco UCS C-Series servers supports a wide variety of 10 Gigabit Ethernet connectivity options using Cisco 10GBASE SFP+ modules.

Table 3: Controllers and SFP+ Twinax Transceivers Support Matrix

Controllers (LOM and PCIe)	10GBASE-CU SFP+ Cable 1 Meter, passive	10GBASE-CU SFP+ Cable 3 Meter, passive
	SFP-H10GB-CU1M	SFP-H10GB-CU3M
Cisco UCS Virtual Interface Cards	x	x

Intel x520		
Broadcom 57712	x	x

Controllers (LOM and PCIe)	10GBASE-CU SFP+ Cable 5 Meter, passive	10GBASE-CU SFP+ Cable 7 Meter, active	10GBASE-CU SFP+ Cable 10 Meter, active
	SFP-H10GB-CU5M	SFP-H10GB-ACU7M	SFP-H10GB-ACU10M
Cisco UCS Virtual Interface Cards	x	x	x
Intel x520			
Broadcom 57712	x	x	x

Table 4: Controllers and SFP+Optical Transceivers Support Matrix

Controllers (LOM and PCIe)	Intel SR Optics	JDSU (PLRXPL-SC-S43-22-N) SFP+	Cisco SFP-10G-SR
Cisco UCS Virtual Interface Cards	NA	NA	x
Intel x520	x	NA	NA
Broadcom 57712	NA	x	x

Firmware Upgrade Details

Firmware Files

The C-Series software release 3.0(2) includes the following software files:

CCO Software Type	File name(s)	Comment
Unified Computing System (UCS) Server Firmware	ucs-c240m4-huu-3.0.2.iso ucs-c220m4-huu-3.0.2.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.3.0.2.iso	Drivers
Unified Computing System (UCS) Utilities	ucs-cxxx-utils-efi.3.0.2.iso ucs-cxxx-utils-linux.3.0.2.iso ucs-cxxx-utils-vmware.3.0.2.iso ucs-cxxx-utils-windows.3.0.2.iso	Utilities

Note Always upgrade the BIOS, the Cisco IMC and CMC from the HUU ISO. Do not upgrade individual components (only BIOS or only Cisco IMC 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 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 Software Features

The following new software features are supported in Release 3.0(2):

- **Key Management Interoperability Protocol**— Support for Key Management Interoperability Protocol (KMIP). KMIP is a communication protocol that defines message formats to handle keys or classified data on a key management server. KMIP is an open standard and is supported by several vendors. Key management involves multiple interoperable implementations, so a KMIP client works effectively with any KMIP server.

Self-Encrypting Drives(SEDs) contain hardware that encrypts incoming data and decrypts outgoing data in realtime. A drive or media encryption key controls this function. However, the drives need to be locked in order to maintain security. A security key identifier and a security key (key encryption key) help achieve this goal. The key identifier provides a unique ID to the drive.

Different keys have different usage requirements. Currently, the responsibility of managing and tracking local keys lies primarily with the user, which could result in human error. The user needs to remember the different keys and their functions, which could prove to be a challenge. KMIP addresses this area of concern to manage the keys effectively without human involvement.

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.

Open Caveats

The following section lists open caveats.

Open Caveats in Release 3.0(2b)

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

Table 5: 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)

Table 6: Utilities

Defect ID	Symptom	Workaround	First Affected Release
CSCvc58466	When you update the server firmware using the **update-all** option of HUU, the Fusion IO 6400 G firmware is not updated. However, HUU's verify update status indicates that the firmware is updated.	None.	3.0(2b)

Table 7: Web Management

Defect ID	Symptom	Workaround	First Affected Release
CSCvc56390	While accessing Cisco IMC web UI using Google Chrome or Microsoft Edge browsers, some of the options in the drop-down menu do not appear as expected.	Use Microsoft Internet Explorer or Mozilla Firefox browser.	3.0(2b)

Table 8: XML API

Defect ID	Symptom	Workaround	First Affected Release
CSCvc25363	Unable to hide or unhide virtual drives using XML API.	Use Cisco IMC web UI or CLI.	3.0(2b)

Open Caveats in Release 3.0(1c)

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

Table 9: 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 10: 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 11: 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)

Defect ID	Symptom	Workaround	First Affected Release
CSCvc45069	While updating the firmware components using Non Interactive HUU, the update may fail with the error message - `Firmware update failed for CIMC, Error - Operation failed. The current operation failed. CIMC may be running any critical operation or in error state. Retry after sometime or reboot CIMC if necessary.` This happens because of an incomplete firmware update triggered previously.	Move the mapped older ISO file from the mounted location in the file share server (nfs/cifs/www) used. Re-initiate the NIHUU update. Alternatively, use the Interactive HUU update method to update the firmware components.	3.0(1c)

Open Caveat in Release 2.0(13h)

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

Table 12: 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 13: BIOS

Defect ID	Symptom	Workaround	First Affected Release

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)
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)
CSCux47767	The C220 M4 and C240 M4 servers might become unresponsive during BIOS posting while configuring the platform hardware. This happens when one of the PCIe devices stops responding due to Option ROM shadowing.	Soft-boot the server from the KVM console.	2.0(13e)
CSCva96780	A server with multiple adapters may fail to boot and appears in the BIOS setup menu. This happens on the first boot up after the placement policy is changed (when the vNIC placement policy is changed between the adapters).	Perform a warm reboot.	2.0(13e)

Table 14: BMC

Defect ID	Symptom	Workaround	First Affected Release
CSCuz43263	On the C240 M4 servers, the HDDs hosted by the Cisco HBA controllers are displayed a little late in the **piddump** output. This occurs immediately after the blades are powered on.	Wait for two minutes for the HDDs to display.	2.0(13e)
CSCuz61163	After upgrading the server firmware to 2.0(13e), the P1_THERMTRIP & P2_THERMTRIP sensors assertion critical events and deassertion events might be seen in the System Event Log. These are events are not valid and can be ignored.	None.	2.0(13e)

Table 15: External Controllers

Defect ID	Symptom	Workaround	First Affected Release
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)
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)
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)
CSCva93943	Foreign configuration import fails when a drive group is set to transport ready state and a partial set of drives are removed from the system and re-inserted back into the same system, followed by a system reboot.	Manually create or recreate the foreign configuration.	2.0(13e)
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)
CSCva53443	Qlogic 8442T ISCSI LUN is not visible during SLES 12.1 Installation. This happens when the LUN has an inbox driver (version 2.7.6.2) for ISCSI.	None.	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)
CSCva80462	The Intel X710 adapter MAC address is displayed as "000000000000". This happens when the system has two Intel X710 cards, one Intel i350 mLOM adapter, and one Intel i350 LOM, and you enable OptionROMs for all these adapters.	Disable the OptionROM for the Intel i350 LOM or Intel i350 mLOM adapter cards.	2.0(13e)
CSCvb26014	Occasionally, if you boot to HUU and wait for approximately 40 minutes, at the "License Agreement" screen, several entries about currently missing devices are written to the system log (and filtered to the OBFL).	Complete upgrading HUU and exit from the utility.	2.0(13e)
CSCvb24327	When more than 20 drives are zoned to a server while the server is online, it takes a long time (a maximum of 7 minutes) for the drives to be discovered and displayed.	None.	2.0(13e)

CSCva61275	On activating the firmware on SSDs, the following critical error is displayed: `Controller X on server X is inoperable. Reason: CIMC didn't detect storage controller` This happens when you activate the following following models of HGST NVMe SSDs: • UCSC-F-H38001 • UCS-PCI25-38001 This issue occurs because the active slot firmware on the NVMe SSD reverts to the firmware present on the read-only slot. If the firmware on the read only slot does not support Out-Of-Band, this NVMe is not reported in the Out-Of-Band inventory stage and results in the Cisco IMC becoming unresponsive.	None.	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)

Table 16: 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)

Open Caveats in Release 2.0(10b)

The following defects are open in release 2.0(10b):

Table 17: BIOS

Defect ID	Symptom	Workaround	First Affected Release
CSCux01460	After you perform a power characterization, under advance power profile it displays an incorrect power range to cap the memory. This results in ineffective memory domain power capping.	Run the platform power capping instead.	2.0(10b)
CSCuy42471	In cases when TPM is not available, the SIMBIOS OEM table is populated indicating that TPM is present.	None.	2.0(10b)

Table 18: VIC

Defect ID	Symptom	Workaround	First Affected Release
CSCuy23450	On a UCS C-Series server managed using Cisco IMC standalone (not managed by UCS Manager), network connections to Cisco IMC may fail because the IP address assigned to Cisco IMC is not reachable on the IP network. This problem affects servers when a Cisco UCS VIC adapter 1385 or 1387 is used to access Cisco IMC (NIC mode: "Cisco Card") and the VIC adapter uplinks are configured in NIV mode.	Unselect VN-Tag mode and select Classical Ethernet mode.	2.0(10b)

Open Caveats in Release 2.0(9c)

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

Table 19: 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)

Table 20: VIC

Defect ID	Symptom	Workaround	First Affected Release
CSCuv42027	The Priority Flow Control (PFC) mode is always set to 'Standard' on the Cisco VIC adapter if the corresponding switchport's PFC mode is set to ON. This results in the PFC mode not being enabled.	Set the switchport's PFC mode to 'Auto'.	2.0(9c)
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 21: Cisco IMC

Defect ID	Symptom	Workaround	First Affected Release
CSCul95481	The DIMM temperature sensors are not displayed in the Web UI or CLI interfaces.	No workaround. However, use raw IPMI commands to access these sensor readings, which are located in the Cisco Extended SDR.	2.0(4c)

Table 22: 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 23: LOM

Defect ID	Symptom	Workaround	First Affected Release
CSCun71765	The 10GE LOM port (X540 based) flaps when the host reboots while the CIMC is in Shared LOM 10G network mode. This event may drop connections to the CIMC including the Virtual Media and vKVM. • CIMC network mode is Shared LOM 10G • Host reset 10GE LOM PHY. Usually happens on host reboot, driver load/unload or speed change	Do not use Shared LOM 10G network mode if using Virtual Media or vKVM during host boot.	2.0(4c)

Table 24: 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 25: Cisco IMC

Defect ID	Symptom	Workaround	First Affected Release
CSCuq11190	Slow network performance between VMs in OVM 3.3.1.	None.	2.0(3d)

Table 26: 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)
CSCup51154	The HII interface for 9300 is blank when 9300 external LSI adapter is present and ROM mode option is enabled.	None.	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)

Known Behaviors

The following section lists known behaviors.

Known Behaviors in Release 3.0(1c)

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

Table 27: 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 28: 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 29: 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 30: 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 31: 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 32: 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 33: 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 34: 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 35: 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 36: 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 37: 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 38: 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 39: 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(10e)

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

Table 40: 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 41: 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(9c)

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

Table 42: 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 43: 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 44: 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 45: 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 46: 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 47: 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 48: 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 49: 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 50: 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 51: 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 52: 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(6d)

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

Table 53: 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 54: 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 55: 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 56: 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 57: 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 58: 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 59: 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 60: 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 61: 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 62: 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 63: 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)

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