Release Notes for Cisco UCS C-Series Software, Release 1.4(3)

First Published Date: March 14, 2012
Revised Date: August 01, 2018
Part Number: OL-26648-01

This document describes the new features, system requirements, open caveats and known behaviors for C- series software release 1.4(3) 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 on page 58.

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

Table 1 shows the online change history for this document.

Table 1 Online History Change

Part Number	Revision	Date	Description
OL-26648-01	A0	14-March-2012	Created release notes for Release 1.4(3)
	B0	26-March-2012	Revised Host Upgrade Utility (HUU) version to 1.4(3c)1 for change in firmware on UCS P81E The Utilities ISO has been modified for Windows and Linux OS. An EFI ISO has also been introduced.
	C0	12-April-2012	Revised Host Upgrade Utility (HUU) version to 1.4(3c)2 for change in firmware on UCS P81E and to include defect fixes.

Part Number	Revision	Date	Description
	D0	11-May-2012	The following changes were made: • Revised Host Upgrade Utility (HUU) version to 1.4(3j) • Revised CIMC version to 1.4(3j) • Revised BIOS version to 1.4.3f.0 (for C200) and 1.4.3d.0 (for C460, C250, and C250) • Added Release 1.4(3j) to Resolved Caveats section. • Added Release 1.4(3j) to Known Behaviors section
	E0	22-June-2012	The following changes were made: • Revised CIMC and HUU to 1.4(3l) for C260 and C460, and 1.4(3k) for C200, C210 and C250. • Revised BIOS version for C260 and C460 • Changed versions of Broadcom 5709 and LSI 9240-8i adapters • Added Release 1.4(3l) to Resolved Caveats section. • Added Release 1.4(3k) to Resolved Caveats section.
	F0	11-September-2012	The following changes were made: • The 1.4(3p) patch introduces support for Microsoft Windows 2012 on C200, C210 and C250 servers. Virtual Interface Card (VIC) is not supported with Microsoft Windows 2012 OS. • Revised CIMC and HUU version to 1.4(3p) for C200, C210 and C250 servers. • Added Release 1.4(3p) to Resolved Caveats and Known Behaviors sections.
	G0	19-November-2012	The following changes were made: • Revised Host Upgrade Utility (HUU) version to 1.4(3p)5 for C200, C210, and C250 servers. • Updated Resolved Caveats section.
	H0	15-March-2013	The following changes were made: • Revised Host Upgrade Utility (HUU) version to 1.4(3s) for C200 and C250 servers. • Updated the Resolved Caveats section.

Part Number	Revision	Date	Description
	I0	01-May-2013	The following changes were made: • Revised Host Upgrade Utility (HUU) version to 1.4(3s)4 for C200 and C250 servers. • The LSI firmware versions for C200 and C250 servers have been updated. • Updated the Known Behaviors section.
	J0	04-June-2013	The following changes were made: • Revised Host Upgrade Utility (HUU) version to 1.4(3t) for C200 and C250 servers. • Updated the Resolved Caveats section.
	K0	15-August-2013	The following changes were made: • Revised Host Upgrade Utility (HUU) version to 1.4(3u) for C200 and C250 servers. • Updated the Resolved Caveats section.
	L0	24-February-2014	The following changes were made: • Revised Host Upgrade Utility (HUU) version to 1.4(3v) for C200 and C250 servers. • Updated the Resolved Caveats section. • Updated the Open Caveats section.
	M0	26-September-2014	The following changes were made: • Revised Host Upgrade Utility (HUU) version to 1.4(3w) for C200 and C250 servers. • Updated the Resolved Caveats section.
	N0	25-November-2014	The following changes were made: • Revised Host Upgrade Utility (HUU) version to 1.4(3x) for C200 and C250 servers. • Updated the Resolved Caveats section.
	O0	July 02, 2015	Added references to the Cisco UCS Manager release notes and the Cisco UCS C Series Server Integration with Cisco UCS Manager documentation.
	P0	August 17, 2015	Updated the **System Requirements** section with Java compatibility information.

Part Number	Revision	Date	Description
	Q0	November 30, 2015	The following changes were made: • Updated Features in this Release section. • Revised Host Upgrade Utility (HUU) version to 1.4(3x) for C200 and C250 servers. • Updated the Resolved Caveats section.
	R0	December 03, 2015	The following changes were made: • Updated Features in this Release section. • Revised Host Upgrade Utility (HUU) version to 1.4(3y). • Updated the Resolved Caveats section.
	S0	February 27, 2017	The following changes were made: • Updated the Security Fixes section. • Revised Host Upgrade Utility (HUU) version to 1.4(3z) for C200 and C250 servers.
	T0	December 19, 2017	The following changes were made: • Updated the Security Fixes section. • Updated the Resolved Caveats section. • Revised Host Upgrade Utility (HUU) version to 1.4(3z07) for C200 and C250 servers.
	U0	April 06, 2018	The following changes were made: • Updated the Security Fixes section. • Revised Host Upgrade Utility (HUU) version to 1.4(3z08) for C200 and C250 servers.
	V0	August 01, 2018	The following changes were made: • Updated the Security Fixes section. • Revised Host Upgrade Utility (HUU) version to 1.4(3z09) for C200, 210 and C250 servers.
	W0	August 29, 2018	Updated the Security Fixes section for Release 1.4(3z09).

Contents

This document includes the following sections:

Introduction

This section includes the following topics:

Overview of the Servers

Cisco® UCS C-Series Rack-Mount Servers extend unified computing innovations to an industry-standard form factor to help reduce total cost of ownership (TCO) and increase business agility. Designed to operate both in standalone environments and as part of the Cisco Unified Computing

System™1, the series employs Cisco technology to help customers handle the most challenging workloads. The series incorporates a standards-based unified network fabric, Cisco VN-Link virtualization support, and Cisco Extended Memory Technology. It supports an incremental deployment model and protects customer investments with a future migration path to unified computing.

The Cisco UCS C460 High-Performance Rack-Mount Server is designed with the performance and reliability to power compute-intensive, enterprise-critical standalone applications and virtualized workloads. The system is a four-rack-unit (4RU) rack-mount server supporting up to four Intel Xeon 7500 series processors, up to 512 GB of DDR3 memory in 64 slots, and 12 small form-factor (SFF) hot-pluggable SAS and SATA disk drives. Abundant I/O capability is provided by 10 PCI Express (PCIe) slots supporting the Cisco UCS C-Series network adapters, with an eleventh PCIe slot reserved for a hard disk drive array controller card. Additional I/O is provided by two Gigabit Ethernet LAN-on-motherboard (LOM) ports, two 10 Gigabit Ethernet ports, and two dedicated out-of-band (OOB) management ports.

The Cisco UCS C260 High-Performance Rack-Mount Server is designed with the performance and reliability to power compute-intensive, enterprise-critical standalone applications and virtualized workloads. The system is a two-rack-unit (2RU) rack-mount server supporting up to two Intel Xeon 7500 series processors, up to 1 TB of DDR3 memory in 64 slots, and 16 small form-factor (SFF) hot-pluggable SAS and SATA disk drives. Abundant I/O capability is provided by 7 PCI Express (PCIe) slots supporting the Cisco UCS C-Series network adapters and hard disk drive array controller cards. Additional I/O is provided by two Gigabit Ethernet LAN-on-motherboard (LOM) ports, two optional 10 Gigabit Ethernet LOM ports, and two dedicated out-of-band (OOB) management ports.

This server is shipped from the factory with one pre-installed Cisco Flexible Flash card. The slots for these cards are on the I/O riser.

The Cisco UCS C250 Extended-Memory Rack-Mount Server is a two-socket, two-rack-unit (2RU) rack-mount server featuring patented Cisco Extended Memory Technology. It is designed to increase performance and capacity for demanding virtualization and large-data-set workloads. It also can reduce the cost of smaller memory footprints. This server is built for virtualized workloads in enterprise data centers, service provider environments, and virtual desktop hosting. The system also helps increase performance for large-data-set workloads, including database management systems and modeling and simulation applications. Applications that are memory bound today will benefit by the 384 GB of addressable memory that the Cisco UCS C250 server offers.

The Cisco UCS C210 General-Purpose Rack-Mount Server is a general-purpose, two-socket, two-rack-unit (2RU) rack-mount server housing up to 16 internal small form-factor (SFF) SAS or SATA disk drives for a total of up to 32 terabytes (TB) of storage. The Cisco UCS C210 server is designed to balance performance, density, and efficiency for workloads requiring economical, high-capacity, reliable, internal storage. Based on quad-core Intel® Xeon® 5500 or 5600 series processors, the server is built for applications including virtualization, network file servers and appliances, storage servers, database servers, and content-delivery servers.

The Cisco UCS C200 High-Density Rack-Mount Server is a high-density server with balanced compute performance and I/O flexibility. This price-to-performance optimized two-socket, one-rack-unit (1RU) rack-mount server is designed to balance simplicity, performance, and density for web infrastructure and mainstream data center, small-office, and remote-office applications. Its single-rack-unit size makes it useful for service providers offering dedicated or multi-tenant hosting, and its economical price makes it well suited to the appliance market.

C-series servers are capable of standalone management using Cisco Integrated Management Controller (CIMC), which is an integration of the service processor hardware and the CIMC firmware. CIMC has a Web GUI and a CLI mode.

The Cisco UCS C200 M2 Small Form Factor (SFF) server is a factory-configurable option that is an alternate to the existing Cisco UCS C200 M2 Large Form Factor (LFF) server.

The LFF version of the server can contain up to four 3.5-inch LFF hard drives or solid state drives. If a customer orders the new SFF version of the server, the chassis is configured with a drive backplane and front drive bays that can contain up to eight 2.5-inch SFF drives. The drive bays and backplane are factory-configurable, but are not supported as field-configurable.

The SFF server also allows configurable selection of front-panel control modules. Customers can choose the standard control panel module or an optional DVD-drive module. These two modules are field-replaceable and interchangeable with the supplied cables.

In addition, 2.5-inch drives have been qualified as configurable options for the SFF server. The RAID controller options have also been qualified for the SFF server (LSI MegaRAID 9280-4i4e and LSI 1068-based mezzanine card).

Overview of the Pre-Installed Cisco Flexible Flash Card

The Cisco Flexible Flash card is pre-installed with three software bundles, each on one of four preconfigured virtual drives (VDs). The fourth VD allows you to install an OS or an embedded hypervisor.

The VDs are configured with the following content:

- Cisco UCS Server Configuration Utility (SCU).
- Hypervisor (HV). This is a VD that you can use for your own purposes.
- Cisco Drivers (Drivers).
- Cisco Host Upgrade Utility (HUU).

Refer to the following documents for more information about these tasks:

- Replacing a card: *Cisco UCS C260 Server Installation and Service Guide*
- Enabling and booting a VD: *Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide* or the *Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide*
- Monitoring and managing a card with CIMC: *Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide* or the *Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide*

The links to these documents are in the C-Series documentation road map:

http://www.cisco.com/go/unifiedcomputing/c-series-doc

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

Transceivers Specifications

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

Table 2 and Table 3 details the controllers and the supported transceivers.

Table 2 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	10GBASE-CU SFP+ Cable 5 Meter, passive	10GBASE-CU SFP+ Cable 7 Meter, active	10GBASE-CU SFP+ Cable 10 Meter, active
	SFP-H10GB-CU1M	SFP-H10GB-CU3M	SFP-H10GB-CU5M	SFP-H10GB-ACU7M	SFP-H10GB-ACU10M
Cisco UCS P81E VIC	x	x	x	x	x
Qlogic 8152	x	x	x	x	x
Intel x520	x	x	x	x	x
Emulex OCe10102	x	x	x	x	x
Broadcom 57711	x	x	x	x	x
Broadcom 57712	x	x	x	x	x

Table 3 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 P81E VIC	NA	NA	x
Qlogic 8152	NA	NA	No support
Emulex OCe10102	NA	NA	x
Intel x520	x	NA	No support
Broadcom 57711	NA	x	x
Broadcom 57712	NA	x	x

Firmware Files

The C-Series software release 1.4(3) includes the following software files:

Table 4 Files in this release

CCO Software Type	File name(s)	Comment
Unified Computing System (UCS) Server Firmware	ucs-c200-huu-1.4.3z09.iso ucs-c250-huu-1.4.3z09.iso ucs-c260-huu-1.4.3l.iso ucs-c460-huu-1.4.3l.iso	Host Upgrade Utility
Unified Computing System (UCS) Drivers	ucs-cxxx-drivers.1.4.3a.iso	Drivers

Table 4 Files in this release

CCO Software Type	File name(s)	Comment
Unified Computing System (UCS) Utilities	ucs-c2xx-utils-linux.1.4.3a.iso ucs-c2xx-utils-vmware.1.4.3.iso ucs-c2xx-utils-windows.1.4.3a.iso ucs-c2xx-utils-efi.1.4.3.iso	Utilities
Unified Computing System (UCS) Adapter Firmware	ucs-cxxx-fw.1.4.3b.iso	Third-Party Firmware

Note Always upgrade both the BIOS and the CIMC from the HUU ISO. Do not upgrade individual components (only BIOS or only CIMC), since this could lead to unexpected behavior.

Host Upgrade Utility

The Cisco Host Upgrade Utility (HUU) is a tool that upgrades the following firmware:

- Cisco Integrated Management Controller (CIMC)
- System BIOS
- LAN on motherboard (LOM)
- RAID Controllers (LSI storage controllers)
- Cisco UCS P81E Virtual Interface Card (VIC)
- Broadcom PCIe adapters
  - 5709 Dual and Quad port adapters
  - 57711 Dual port adapter
  - 57712 Dual port adapter
- Intel® PRO/1000 PF Quad Port Server Adapter

In addition, this utility now supports the following options:

- Download ISO images for a selected platform on a Windows operating system.
- Recover a corrupt BIOS in the EFI shell.

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

Starting with this 1.4 release, separate ISO images of Host Upgrade Utility are available for different server platforms.

The ISO image is now named as ucs-<server_platform>-huu-<version_number>.iso.

The Cisco Host Upgrade Utility contains the following files:

Table 5 Files in ucs-c200-huu-1.4.3z09.iso

Server(s)	Component	Version
C200M1	CIMC	1.4(3z09)
C210M1	BIOS	1.4.3o.0
C200M2	UCS P81E	2.2(3b) - uboot - 2.2(3b)
C210M2	LOM	
C200M2 SFF	Intel-82576	1.4
	PCIe Adapters	
	Broadcom 5709-Dual-Port	A0907GT7441.0-7.4.0
	Broadcom 5709-Quad-Port	A0906GT7441.0-7.4.0
	Broadcom 57711-Dual-Port	6.2.25
	Broadcom 57712-Dual-Port	A1213GT7441.0
	Intel® PRO/1000 PF Quad Port Server Adapter	1.3.32
	Intel-82576-Quad-Port	1.3.32
	LSI	
	1064	1.32.09.00
	1068	1.32.09.00
	8708	1.40.272-1225
	9260-4i	2.130.363-2183
	9260-8i	2.130.363-2183
	9261-8i	2.130.363-2183
	9280-4i4e	2.130.363-2183

Table 6 Files in ucs-c250-huu-1.4.3z09.iso

Server(s)	Component	Version
C250M1	CIMC	1.4(3z09)
C250M2	BIOS	1.4.3n.0
	UCS P81E	2.2(3b) - uboot - 2.2(3b)
	LOM	
	Broadcom 5709	6.0.0
	PCIe Adapters	
	Broadcom 5709-Dual-Port	A0907GT7441.0-7.4.0

Table 6 Files in ucs-c250-huu-1.4.3z09.iso (continued)

Server(s)	Component	Version
	Broadcom 5709-Quad-Port	A0906GT7441.0-7.4.0
	Broadcom 57711-Dual-Port	6.2.25
	Broadcom 57712-Dual-Port	A1213GT7441.0
	Intel® PRO/1000 PF Quad Port Server Adapter	1.3.32
	Intel-82576-Quad-Port	1.3.32
	LSI	
	3081	1.32.09.00
	9261-8i	2.130.363-2183

Table 7 Files in ucs-c260-huu-1.4.3l.iso

Server(s)	Component	Version
C260M2	CIMC	1.4(3l)
	BIOS	1.4.3f.0
	UCS P81E	2.0(2i) - uboot - 2.0(2i)
	LOM	
	Broadcom 5709	C260T6441-4.5
	Broadcom 57712	C260T6444-4.11
	8727-Phy	aa0.511
	PCIe Adapters	
	Broadcom 5709-Dual-Port	6.0.0
	Broadcom 5709-Quad-Port	6.0.0
	Broadcom 57711-Dual-Port	6.2.15 - aa0.406
	Broadcom 57712-Dual-Port	A1213GT6444.0
	Broadcomm 57712-10G-BaseT	A1202GT6441.0
	INTEL-82576-Quad-Port	1.3.32
	LSI	
	926x	2.120.233-1471

Table 8 Files in ucs-c460-huu-1.4.3l.iso

Server(s)	Component	Version
C460M1	CIMC	1.4(3l)
C460M2	BIOS	1.4.3e.0
	UCS P81E	2.0(2i) - uboot - 2.0(2i)
	LOM	
	Broadcom 5709	C460T6045-2.0
	Broadcom 57711	C460T6045-2.0
	Broadcom 57711- phy	3.3/aa0.5ad
	PCIe Adapters	
	Broadcom 5709-Dual-Port	6.0.0
	Broadcom 5709-Quad-Port	6.0.0
	Broadcom 57711-Dual-Port	6.2.15 - aa0.406
	Broadcom 57712-Dual-Port	A1213GT6444.0
	Broadcomm 57712-10G-BaseT	A1202GT6441.0
	Intel® PRO/1000 PF Quad Port Server Adapter	1.3.32
	LSI	
	9260-8i	2.120.233-1471
	9240-8i	2.120.274-1543

Note The introduction of the new firmware for UCS P81E resolves the problem of Microsoft Windows 2008 bare metal hosts losing all network configuration information and recording a numbering shift in the NICs after an upgrade. This problem occurs only after upgrading the UCS P81E firmware to 2.0(2h). Upgrading the firmware of the UCS P81E VIC to 2.0(2i) retains the pre-upgrade NIC configuration.

System Requirements

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

- Sun JRE 1.7.0_45 or earlier (Till 1.6.0_14)
- Microsoft Internet Explorer 6.0 or higher, Mozilla Firefox 3.0 or higher
- Microsoft Windows 7, Microsoft Windows XP, Microsoft Windows Vista, Apple Mac OS X v10.6, Red Hat Enterprise Linux 5.0 or higher operating systems

Updating the Firmware

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

- BIOS
- CIMC
- LAN on Motherboard Settings
- RAID Controller Firmware
- Select PCIe adapter Firmware

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

Features in this Release

This section includes the following topics:

Supported Features

Supported Operating Systems in Release 1.4(3y)

Support to the following Operating Systems were added for this release:

- VMware ESXi 5.0 Update 3
- VMware ESXi 5.1 Update 3
- VMware ESXi 5.5 Update 2
- VMware ESXi 5.5 Update 3
- VMware ESXi 6.0
- VMware ESXi 6.0 Update 1
- Windows Server 2012 R2
- Red Hat Enterprise Linux Versions 6.5, 6.6 and 6.7
- Red Hat Enterprise Linux Versions 7.0 and 7.1

Features in Release 1.4(3u)

- BIOS changes

  The BIOS image with this release contains the Microcode Update which fixes the Intel VT FlexPriority Errata which is documented in the Intel Public Spec Update for Aug 2013. This errata impacts all Cisco UCS C-series servers.

Supported Features in Release 1.4(3)

The following features were introduced in the Release 1.4(3):

- Support for UCS Manager in C200 M2, C210 M2, C250 M2, C260 M2, and C460 M2 server platforms.
- Availability of CIMC tech support information that can be downloaded from the browser.
- Support for CIMC system log filtering and availability of improved message severity.
- Availability of CIMC SNMP v3 as the default mode for SNMP which improves security.
- Improved CIMC SEL messages.
- Availability of new options like CPU, DIMM, HDD, and PCI Product ID (PID) in the CIMC CLI commands.
- Synchronization of CIMC clock with the system real-time clock when CIMC boots.
- SEL fullness information.

Supported Platforms

The following platforms are supported in release 1.4(3):

- UCS-C200
- UCS-C210
- UCS-C250
- UCS-C260
- UCS-C460

SNMP

The supported MIB definition for release 1.4(3) 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.

Supported Storage Controllers

SNMP supports the following storage controllers:

- 9260-4i
- 9260-8i
- 9261-8i
- 9240-8i
- 9280-4i4e

BIOS and Hardware

Symptom Cisco is introducing a new generation of SATA 2.5-inch hard drives which are for the first time compatible with the new SATA Revision 3.0 standard capable of 6 Gbit/s. In particular these hard drives are SATA 500 GB (A03-D500GC3) and 1 TB (A03-D1TBSATA). Due to legacy design constraints in certain Generation M2 C-Series servers, the faster 6 Gbit/s link speeds may not always be possible in all servers. However, in those cases, the link speeds will properly negotiate the link back to the Revision 2.0 standard capability of 3 Gbit/s. This operation is seamless to the user.

Workaround This is a known behavior, as follows:

- The UCS C200 M2 SFF server supports these drives at full 6Gbit/s speeds.
- The UCS C210 M2 server guarantees support of these drives at a minimum of 3Gbit/s speeds.
- The UCS C250 M2 server guarantees support of these drives at a minimum of 3Gbit/s speeds.
- The UCS C460 server supports these drives at full 6Gbit/s speeds.
- The UCS C260 server supports these drivers at full 6Gbit/s speeds.

Note In some cases, you may find that some or all links have negotiated to the higher 6Gbit/s speeds. Those links that do, will operate properly at that speed.

Upgrading BIOS and CIMC firmware

Caution When you upgrade the BIOS firmware, you must also upgrade the CIMC firmware from the same HUU ISO, or the server may not boot. Do not power off the server until the BIOS and CIMC firmware are updated.

Cisco provides the Cisco Host Upgrade Utility to assist you in upgrading the BIOS, CIMC, LOM, LSI storage controller, and Cisco UCS P81E Virtual Interface Card firmware to compatible levels.

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

To use this utility, start with the Cisco Host Upgrade Utility User Guide, which includes the instructions for downloading and using the utility ISO. Select the correct guide for your desired firmware version from this URL:

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

- Cisco Host Upgrade Utility User Guide for Release 1.2(x)
- Cisco Host Upgrade Utility User Guide for Release 1.3(x)
- Cisco Host Upgrade Utility User Guide for Release 1.4(x)

Security Fixes

Release 1.4(3z09)

The following security fixes were applied in Release 1.4(3z09):

Release	Defect ID	CVE ID	Symptom
1.4(3z09)	CSCvm02934	• CVE-2018-3615 • CVE-2018-3620 • CVE-2018-3646	Cisco UCS C-Series M2 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 M2 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 ID	Symptom
1.4(3z09)	CSCvj59309	• CVE-2018-3639 • CVE-2018-3640	Cisco UCS M2 servers are based on Intel® EP Series 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 M2 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). For more information, please see the Cisco Security Advisory at: CPU Side-Channel Information Disclosure Vulnerabilities: May2018

Release 1.4(3z08)

The following security fixes were applied in Release 1.4(3z08):

Release	Defect ID	CVE ID	Symptom
1.4(3z08)	CSCvh31576	• CVE-2017-5715 • CVE-2017-5715 • CVE-2017-5754	Cisco UCS and Hyperflex 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. • Cisco UCS and Hyperflex 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-2017-5754 (Meltdown) is addressed by applying the relevant Operating System patches from the appropriate vendors. • CVE-2017-5715 (Spectre/Variant 2) is addressed by applying the updated microcode included in the UCS Manager release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. This release includes BIOS revisions for Cisco UCS M2 generation servers. These BIOS revisions include 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

Release 1.4(3z07)

The following security fixes were applied in Release 1.4(3z07):

Release	Defect ID	CVE ID	Symptom
1.4(3z07)	CSCve86968	CVE-2017-6616	A vulnerability in the web interface of CMC was addressed.

Release	Defect ID	CVE ID	Symptom
	CSCve86938	CVE-2017-6619	A vulnerability in the web interface of CMC was addressed.
1.4(3z08)	CSCvh31576	• CVE-2017-5715 • CVE-2017-5715 • CVE-2017-5754	Cisco UCS and Hyperflex 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. • Cisco UCS and Hyperflex 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-2017-5754 (Meltdown) is addressed by applying the relevant Operating System patches from the appropriate vendors. • CVE-2017-5715 (Spectre/Variant 2) is addressed by applying the updated microcode included in the UCS Manager release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. This release includes BIOS revisions for Cisco UCS M2 generation servers. These BIOS revisions include 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

Release 1.4(3z)

The following security fixes were applied in Release 1.4(3z):

Release	Defect ID	CVE ID	Symptom
1.4(3z)	CSCus42715	CVE-2014-3569, CVE-2014-3570, CVE-2014-3571, CVE-2014-3572, CVE-2014-8275, CVE-2015-0204, CVE-2015-0205, CVE-2015-0206	A vulnerability in OpenSSL has been addressed.
	CSCut45903	CVE-2015-0286, CVE-2015-0287, CVE-2015-0289, CVE-2015-0292, CVE-2015-0293, CVE-2015-0209, CVE-2015-0288	A vulnerability in OpenSSL has been addressed.
	CSCuu82366	CVE-2015-4000, CVE-2015-1788, CVE-2015-1789, CVE-2015-1790, CVE-2015-1792, CVE-2015-1791, CVE-2014-8176	A vulnerability in OpenSSL has been addressed.
	CSCuv26140	CVE-2015-1793	A vulnerability in OpenSSL has been addressed.
	CSCux41335	CVE-2015-3193, CVE-2015-3194, CVE-2015-3195, CVE-2015-3196 and CVE-2015-1794	A vulnerability in OpenSSL has been addressed.
	CSCuy54501	CVE-2016-0800, CVE-2016-0705, CVE-2016-0798, CVE-2016-0797, CVE-2016-0799, CVE-2016-0702, CVE-2016-0703, CVE-2016-0704	A vulnerability in OpenSSL has been addressed.
	CSCuz52406	CVE-2016-2108, CVE-2016-2107, CVE-2016-2105, CVE-2016-2106, CVE-2016-2109, CVE-2016-2176	A vulnerability in OpenSSL has been addressed.
	CSCvb48579	CVE-2016-6304, CVE-2016-6305, CVE-2016-2183, CVE-2016-6303, CVE-2016-6302, CVE-2016-2182, CVE-2016-2180, CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2181, CVE-2016-6306, CVE-2016-6307, CVE-2016-6308, CVE-2016-6309, CVE-2016-7052	A vulnerability in OpenSSL has been addressed.
	CSCvb56137	CVE-2016-7406, CVE-2016-7407, CVE-2016-7408 and CVE-2016-7409	A vulnerability in OpenSSH has been addressed.
	CSCuw08475	CVE-2016-7406, CVE-2016-7407, CVE-2016-7408 and CVE-2016-7409	A vulnerability in OpenSSH has been addressed.
	CSCut95997	CVE-2013-2566, CVE-2015-2808	An RC4 vulnerability has been addressed.
	CSCux22875	CVE-2008-5161	A vulnerability in OpenSSH has been addressed.
	CSCux49987	CVE-2008-5161	A vulnerability in OpenSSH has been addressed.

Release	Defect ID	CVE ID	Symptom
	CSCvb62003	CVE-2016-7406, CVE-2016-7407, CVE-2016-7408 and CVE-2016-7409	A vulnerability in OpenSSH has been addressed.
	CSCvd67938	CVE-2015-0235	A GLIBC GHOST vulnerability has been addressed.

Resolved Caveats

This section includes the following topics:

Release 1.4(3z07)

The following caveat was resolved in 1.4(3z07) release:

BIOS

Symptom After rebooting a C250 M2 server, all DIMMs in one or more channels are disabled and a CIMC fault is generated for each disabled DIMM.

Workaround Power cycle (pull power) the server.(CSCuz50456)

Release 1.4(3y)

The following caveats were resolved in 1.4(3y) release:

CIMC

Symptom The recursive group search with LDAP fails on CIMC and the user is timed out at the login page. (CSCut27618)

BIOS

Symptom The system may fail due to SMBUS traffic collisions (such as false thermal alarms and so on) on the SMBUS shared by the host and BMC.

Workaround No workaround.(CSCuv62987)

Release 1.4(3x)

The following caveats were resolved in 1.4(3x) release:

Symptom The Bash shell is affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2014-6271
- CVE-2014-6277
- CVE-2014-6278

The vulnerabilities identified above are addressed.(CSCur03816)

Symptom The Cisco IMC includes a version of DropBear SSH Server that is affected by the vulnerabilities identified by the Common Vulnerability and Exposures (CVE) CVE-2013-4421. The remote host runs an SSH server that is vulnerable to multiple issues.

The vulnerabilities identified above are addressed.(CSCul56637)

Symptom There are known vulnerabilities in the older versions of the OpenSSL code.

This issue is resolved with the latest CiscoSSL/OpenSSL versions.(CSCup22566)

Symptom The Cisco IMC is affected by an SSLv3 vulnerability identified by the Common Vulnerability and Exposures (CVE) CVE-2014-3566.

The vulnerabilities identified above are addressed.(CSCur33929)

Release 1.4(3w)

The following caveats were resolved in 1.4(3w) release:

CIMC

Symptom For server on versions 1.4(1) or higher, disabling the USB boot using the BIOS boot option does not work. In spite of disabling the USB boot by using the **Make Device Not Bootable** option, you are able to boot from a USB device.

Workaround No workaround.(CSCup59737)

BIOS

Symptom You do not have the BIOS option to choose UEFI only or Legacy only on M2 servers.

Workaround No workaround.(CSCup91677)

Release 1.4(3v)

The following caveats were resolved in 1.4(3v) release:

Symptom Cisco UCS C-200 M2 Servers display incorrect SNMP values (temperature and disk size) when running firmware 1.4(3u).

Workaround Upgrading to CIMC version 1.4(3v) or later resolves the disk size related issues. However, the upgrade will not resolve the temperature related issues for M2 platforms.(CSCul59145)

Symptom To address security issues, on CIMC factory defaults IPMI 1.5 related ciphers will be disabled.

Workaround Use an RMCP+ interface while communicating with CIMC over a LAN or enable the ciphers for your system.

Release 1.4(3u)

The following caveats were resolved in 1.4(3u) release:

Symptom When one PSU is unplugged, CIMC shows PSU redundancy status as lost. However, SNMP PSU status still shows as online.

Workaround None (CSCug60142)

Symptom SNMP traps are sent out with the credentials of “public” in the community string ignoring the actual configured value that is set in the SNMP configuration of the CIMC.

Workaround Upgrading to CIMC version 1.4(3p) or later resolves this issue. (CSCud18215)

Release 1.4(3t)

The following caveats were resolved in 1.4(3t) release:

Symptom The traps send on insertion and removal of HDDs on C210-M2 has wrong severity set. The insertion trap has a severity of 5 (Major) while removal trap has a severity of 0 (Cleared). The expected behavior is that the insertion event should have a lower severity than that of the removal event.

Workaround None (CSCug10954)

Symptom Several KCS and vKCS timeout errors are seen in the CIMC logs.

Workaround None. (CSCue86259)

Symptom Managed and standalone Cisco Unified Computing System (UCS) deployments contain one or more of the vulnerabilities:

- Cisco Unified Computing System LDAP User Authentication Bypass Vulnerability
- Cisco Unified Computing System IPMI Buffer Overflow Vulnerability
- Cisco Unified Computing Management API Denial of Service Vulnerability
- Cisco Unified Computing System Information Disclosure Vulnerability
- Cisco Unified Computing System KVM Authentication Bypass Vulnerability

Workaround Cisco has released free software updates that address these vulnerabilities. These vulnerabilities affect only Cisco UCS. Additional vulnerabilities that affect the NX-OS base operating system of UCS are described in Multiple Vulnerabilities in Cisco NX-OS-Based Products. (CSCug65591)

This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130424-ucsmulti

Release 1.4(3s)

The following caveats were resolved in 1.4(3s) release:

BIOS

Symptom Allow the user to manage the memory refresh rates from the BIOS setup menu.

Workaround None (CSCuf28394)

Symptom Corrupt KVM display when SATA mode is set to AHCI so that additional Option ROMS are not available during POST.

Workaround Change SATA mode to Compatibility mode and then make changes in other Option ROMS. Once changes are made in the Option ROM, go back into the BIOS and set SATA mode to AHCI. (CSCuc22147)

Symptom CPU frequency drops from 2.9ghz to 1600mhz on reboot. Degraded CPU frequency is seen in BIOS, CIMC, and OS /proc/cpuinfo.

Workaround Hard power off/on the server instead of reboot. (CSCub84930)

CIMC

Symptom PSU FAN fault is generated and Redundancy LOST events logged in SEL.

Workaround AC Off to the PSU which shows fan fault will recover the PSU. (CSCue27696)

Symptom With two PSU installed on C250-M2 and AC cords plugged in, when one of the AC cords is unplugged, the CIMC reboots.

Workaround None (CSCud84195)

Release 1.4(3p)5

The following caveat was resolved in 1.4(3p)5 release:

VIC

Symptom Virtual Interface Card (VIC) does not support Microsoft Windows 2012 on C-series server platforms in 1.4(6), 1.4(6d) and 1.4(3p) releases.

Workaround There is no workaround for this issue.

Release 1.4(3p)

The following caveats were resolved in 1.4(3p) release:

BIOS

Symptom On C200 servers, the RAID properties are greyed out in the RAID BIOS.

Workaround Remove the PCI cards, and enter the RAID BIOS. You should be able to configure RAID. (CSCtz63555).

CIMC

Symptom CIMC is unstable, or inaccessible through the CLI, or GUI, or both.

Workaround Reboot the CIMC. If it continues to be inaccessible, re-plug the power cord to restart the CIMC. (CSCub25194).

Symptom The following errors are seen in the logs after upgrading to CIMC 1.4(1c):

BMC:dump_pwrcap:-: pwrcap_util.c:218:[get_max_pstate]Handle CPU model
fBMC:kernel:-:<7>[peci_issue_transaction]:190:peci: bad FCS1, received = 0x0, expected = 0x89
BMC:kernel:-:<7>[peci_issue_transaction]:220:peci: transaction failed: [0x61]
BMC:kernel:-:<7>[peci_issue_transaction]:190:peci: bad FCS1, received = 0x0, expected = 0x85
BMC:kernel:-:<7>[peci_issue_transaction]:220:peci: transaction failed: [0x61]
BMC:kernel:-:<7>[peci_issue_transaction]:190:peci: bad FCS1, received = 0x0, expected = 0x89
BMC:kernel:-:<7>[peci_issue_transaction]:220:peci: transaction failed: [0x61]

Workaround None (CSCtt70269)

Symptom A server may not boot up with an address assigned to its management interface.

Workaround Set CIMC to the default options from the CIMC Configuration Utility. (CSCub02017)

Release 1.4(3l)

The following caveats were resolved in 1.4(3l) release:

CIMC

Symptom A rack server may have some of the POST LEDs switched on during the operation without having any faults or warnings logged in the SEL or syslog.

Workaround None. You can perform the usual troubleshooting techniques to confirm if a problem exists in the server. (CSCtz96125)

BIOS

Symptom In Cisco C260 and Cisco C460 servers, under certain timing conditions involving multiple cores, a cacheable load may appear to be ordered before an earlier cacheable locked instruction that accesses a different location. In some circumstances this could lead to the following unpredictable system behavior:

- The system may stop responding.
- A system operating in a Microsoft Windows environment may generate a blue screen.
- A system operating in a Linux environment may generate a kernel panic.
- A system operating in a VMware ESX environment may generate a Purple Screen of Death (PSoD).
- An application may not function as intended.

Workaround None. (CSCua23894)

Release 1.4(3k)

The following caveats were resolved in 1.4(3k) release:

CIMC

Symptom A rack server may have some of the POST LEDs switched on during the operation without having any faults or warnings logged in the SEL or syslog.

Workaround None. You can perform the usual troubleshooting techniques to confirm if a problem exists in the server. (CSCtz96125)

Release 1.4(3j)

The following caveats were resolved in 1.4(3j) release:

CIMC

Symptom The Data Center Manageability Interface (DCMI) displays the same values for minimum and maximum for various averaging periods as the values observed since the CIMC boot. The averaging for each period is updated only at the end of that period so convergence appears a bit slow on the DCMI management station.

Workaround This issue has been resolved.(CSCty07570)

Symptom In C200 and C210 servers, the power restore policy does not work with the Power Supply Unit R2X0-PSU2-650W-SB to restore the last power state after a power cycle.

Workaround None. The server has to be manually switched on.(CSCty13774)

Symptom In C260 servers, the power restore policy cannot be used to switch on the server after a power cycle.

Workaround None.(CSCty20464)

Symptom The following symptoms are observed:

- CIMC does not detect the PSU failure when the physical PSU is displaying amber light.
- CIMC does not detect the PSU redundancy failure when the physical PSU is failing.

Workaround None. (CSCty50079)

BIOS

Symptom While installing Citrix XenServer 5.6 FP1SP2 with BIOS default setting, the following error message is displayed and the system gets rebooted.

```
(XEN) **************************************
(XEN) Panic on CPU 0:
(XEN) FATAL PAGE FAULT
(XEN) [error_code=0000]
(XEN) Faulting linear address: 0000000000000408
(XEN) **************************************
```

Workaround Before starting the installation, set the BIOS “Hyperthreading” option to disabled. Once the installation is complete, set it back to enabled. (CSCtx67515)

Symptom RAID policies do not get configured on the ICH10R controller which use UCSM.

Workaround After the UCSM association is complete, reset the system and configure the RAID directly using the LSI Option ROM. Be sure that there is no scrub policy in place in the service profile. This prevents the deletion of RAID volumes in subsequent UCSM associations.(CSCtx66152)

Symptom C200 CIMC PSU_REDUNDANCY sensor does not report loss of PSU redundancy when one out of the two PSU is pulled out from the system.

Workaround None.(CSCty56693)

Symptom Disabling or enabling hyperthreading in the BIOS setup on C260 or C460 servers and then saving the BIOS settings with F10 causes BIOS to hang.

Workaround This issue has been resolved.(CSCtz18060)

Symptom vHBAs and other PCI devices may stop responding in ESX/ESXi 4.1 and ESXi 5.0 when using Interrupt Remapping and this may lead to various functional issues like HBAs stop responding, other PCIs devices stop responding and so on.

Workaround Try one of the following workarounds:

- Disable interrupt remapping in BIOS setup under CPU configuration tab.
- Disable interrupt remapping under ESX.

For more information, refer to the following link:
http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1030265

(CSCty96722)

Release 1.4(3)

The following caveats were resolved in the 1.4(3) release:

Host Upgrade Utility

Symptom When upgrading the firmware of the Broadcom 5709 adapter to 5.2.3 using the Host Upgrade Utility, the hardware iSCSI stops working.

Workaround None (CSCty78589)

Symptom After the firmware is updated to the latest package on the 9240-8i cards using HUU, the Cisco specified NVData settings are not enabled. This could cause the system to hang in the LSI Option ROM for user input.

Workaround Enable the Cisco specified NVData settings as follows:

Step 1 Restart the system.

Step 2 Press Control+H when LSI Option ROM is seen during BIOS POST.

Step 3 In the Web BIOS, select Controller Properties from the Menu on the left pane.

Step 4 Click **Next** in the Controller Properties page.

Step 5 Select Yes from the Set factory Defaults drop down list.

Step 6 Click **Hit.**

Step 7 Exit from the Web BIOS utility and restart the server.

The Cisco specified NVDATA settings gets loaded on the 9240-8i card.(CSCty33796)

CIMC

Symptom The C260 and C460 servers displays incorrect mirrored DIMMs.

Workaround Use the BIOS setup to view the DIMMs that are being used as mirror units.(CSCtq79397)

Symptom In C200 servers, when you download the tech-support file from CLI or WebUI, the following behavior is observed:

- You are not prompted with a default name
- You are expected to enter the correct file extension since the file extension conditions are not enforced.

Workaround None.(CSCtg45351)

Symptom The following scenarios are observed in the C200 and C210 platforms:

- The CIMC log messages displays the following:

```
5:2011 Sep 27 13:07:52:BMC:IPMI:584: SanDiego_ECC_Support.c:75: ->
ReadPeciEccRegister: Peci Transaction Failed!  CPU[31].REG[80] RC: 63
5:2011 Sep 27 13:07:52:BMC:IPMI:584: SanDiego_ECC_Support.c:75: ->
ReadPeciEccRegister: Peci Transaction Failed!  CPU[30].REG[80] RC: 63
0:2011 Sep 27 13:07:55:BMC:IPMI:584: Pilot2Peci.c:85:Pilot2_PECI: PECI Temp
Transaction To CPU-1 Failed!  RC: 63
0:2011 Sep 27 13:07:55:BMC:IPMI:584: Pilot2Peci.c:85:Pilot2_PECI: PECI Temp
Transaction To CPU-0 Failed!  RC: 63
0:2011 Sep 27 13:08:01:BMC:IPMI:584: Pilot2Peci.c:85:Pilot2_PECI: PECI Temp
Transaction To CPU-1 Failed!  RC: 63
0:2011 Sep 27 13:08:01:BMC:IPMI:584: Pilot2Peci.c:85:Pilot2_PECI: PECI Temp
Transaction To CPU-0 Failed!  RC: 63
```

- Fans may run at an unusually high speed (>6100 RPM) and displays the following results:

```
W793_FAN1_TACH1  | 6200.000   | RPM        | ok    | 600.000   | 800.000   | na
| na         | na         | na
W793_FAN1_TACH2  | 6300.000   | RPM        | ok    | 600.000   | 800.000   | na
| na         | na         | na
W793_FAN2_TACH1  | 6100.000   | RPM        | ok    | 600.000   | 800.000   | na
| na         | na         | na
W793_FAN2_TACH2  | 6500.000   | RPM        | ok    | 600.000   | 800.000   | na
| na         | na         | na
W793_FAN3_TACH1  | 6200.000   | RPM        | ok    | 600.000   | 800.000   | na
| na         | na         | na
W793_FAN3_TACH2  | 6400.000   | RPM        | ok    | 600.000   | 800.000   | na
| na         | na         | na
```

- CPU temperature sensors (P1_TEMP_SENS/P2_TEMP_SENS) reads as n/a.

Workaround Shut down and restart the server.(CSCtu08709)

Symptom When you are running VMware ESX 4U1 in C250 servers, the CIMC displays the following log:

```
BMC:IPMI:675: mcddI2CDrv.c:860:PI2CPerformOP: ioctl to driver failed to read
Bus[5].Dev[c0]!  ErrorStatus[32]
```

Workaround None.(CSCtw66408)

Symptom The critical events logged by CIMC for voltage sensors in C250 servers are displayed as follows:

```
P0V75_DDR3_P2: Voltage sensor, failure event, Lower Critical going low (0.672 < 0.672 V)
was asserted
P0V75_DDR3_P2 #0x12 | Critical | Upper critical - going high | Asserted | Reading 0.79 >
Threshold 0.78 Volts
Voltage P1V5_DDR3_P2 #0x09 | Critical | Upper critical - going high | Asserted | Reading
1.56 > Threshold 1.56 Volts
FRU_RAM P5V_SCALED: Voltage sensor for FRU_RAM, failure event, Lower Critical going low
(4.748 < 4.748 V) was asserted
FRU_RAM P1V8_IOH: Voltage sensor for FRU_RAM, failure event, Upper Critical going high
(1.908 > 1.908 V) was asserted
```

Workaround None.(CSCtw93554)

Symptom You are not able to access the CIMC page of the C210 M2 server and a “Error 2001: Service unavailable" error message is observed.

Workaround Perform the following steps:

Step 1 Reset CIMC to the factory default value. The UUID should display 000000.

Step 2 Change the system to ‘dedicated’ from ‘shared LOM’ so that it uses the same IP address.

Step 3 Reset CIMC.

Step 4 Reset BIOS to boot at Extensible Firmware Interface (EFI).

Step 5 Shut down and restart the server.(CSCtx42549)

Symptom The CIMC log does not display messages with the following log severity like:

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Informational
- Debug.

Workaround None.(CSCtu46321)

Symptom When you remove a hard drive and insert a new one, the CIMC Web GUI and CLI shows Slot 0 as a blank row and no information is displayed for the new inserted drive.

Workaround This issue has been resolved.(CSCto35180)

Symptom If you create a RAID 10 or RAID 1 drive group with more than four hard disks, the RAID group is displayed as "Unknown" in the CIMC Web GUI and CLI.

Workaround This issue has been resolved.(CSCto35353)

Symptom A large number of System Event Log (SEL) messages are observed when CIMC is initializing. This includes messages for entities (for example, HDDs) that are not present in the system and their corresponding LEDs states.

Workaround This is an expected behavior. During initialization, the SEL messages are filtered so that the absent entities and their LED states are not displayed. The SEL messages are not filtered after the CIMC is completely initialized.(CSCtt38577)

Symptom SEL messages with the following description were observed:

```
Predictive failure deasserted was asserted
```

Workaround The description has been changed as follows:

```
Predictive failure deasserted
```
(CSCtu07831)

Symptom The CIMC Storage Management CLI displays invalid or no information.

Workaround The CIMC Storage Management CLI now has the following two fields:

- Info Valid—Displays if information is valid. It has two options -Yes or No
- Info Invalid cause—Displays the reason for invalidity if the Info Valid option is No.(CSCtu09166)

Symptom When a drive is removed from a RAID group such as RAID 1 or RAID 10 and reinserted after a few minutes, the drive status under the Physical Drive shows "Unconfigured Bad" while the status in Virtual drive tab shows "Unknown".

Workaround The physical drive that is removed and reinserted now shows the Virtual drive tab status as “Missing” because the drive is “Unconfigured Bad” and is not part of the RAID group.(CSCtu45159)

Symptom The Web-Services Management (WSMAN) and System Management Architecture for Server Hardware Command Line Protocol (SMASH CLP) interfaces are not active.

Workaround The WSMAN and SMASH CLP interfaces have been replaced with the local Web GUI, local CLI, and XML programmatic interfaces.(CSCtu77680)

Symptom The Predictive Failure Count generated by the hard disk is not updated dynamically in the CIMC Web GUI and CLI storage page. The CIMC needs to be rebooted to get the latest Predictive Failure Count.

Workaround This issue has been resolved.(CSCtw84977)

Symptom When you remove a hard disk from the slot and navigate to the Physical tab in the Storage page in CIMC Web GUI, an error dialog box displays and the missing drive is displayed as “Unknown” in the Physical Drive list.

Workaround This issue has been resolved.(CSCtw87968)

Symptom When a physical drive goes offline, the drive state in the CIMC Web GUI displays “Offline” but the Fault displays as “false”.

Workaround This issue has been resolved. The Fault state displays “true” for offline physical drives.(CSCtx06713)

Symptom After the battery learn cycle, the Virtual Drive Cache policy displays Writethrough mode in the CIMC Web GUI and CLI.

Workaround The Virtual Drive Cache policy changes to Writeback mode after the battery learn cycle.(CSCtx20447)

Symptom If you want to download the technical support file from CIMC by using **Admin > Utilities > Tech Support Details,** you will need a Trivial File Transfer Protocol (TFTP) server for downloading.

Workaround None.(CSCtg87868)

Symptom The output for a AAA logout from the CIMC returns a response without the closing quote after the cookie ID. The malformed response is as follows:

```
<aaaLogout cookie="1329308956/dc2c0bc0-b8ff-18ff-8005-03981d0fdf1c response="yes"
outStatus="success">
```

Workaround None.(CSCtu16624)

Symptom The C260 M2 and C460 M2 servers are not supported by UCS Manager.

Workaround None.(CSCtn76680)

Symptom The CIMC Web UI cannot create, modify, or delete P81E VIC vHBAs.

Workaround Use the CIMC CLI to create, modify, or delete P81E VIC vHBAs.(CSCts17797)

Symptom When CIMC starts, vKVM and vMedia fails to start.

Workaround Restart the CIMC.(CSCtx22011)

Symptom A Cisco C200 or C210 rack server may have a "Disturbingly high number of I2C errors" message in the systems logs; when the installed OS is ESXi 4.1 or ESXi 5.0.

Workaround None known at this time. (CSCtt70347)

Symptom Broadcom adapters and LOMs based on BCM5709, BCM57711 and BCM57712 configured for iSCSI and FCoE boot, iSCSI and FCoE boot configuration is lost after firmware upgrade. This is observed in the following cases:

- Using a Broadcom adapter based on BCM5709, BCM57711 or BCM57712.
- Having either iSCSI boot or FCoE boot configuration in the option ROM.
- Upgrading the firmware with HUU.

Workaround Record the configuration before the firmware upgrade and reapply it after the upgrade. (CSCtr85387)

Symptom KVM console fails to launch and displays the following Java exception error:

```
Certificate has been revoked
sun.security.validator.ValidatorException: PKIX path validation failed:
java.security.cert.CertPathValidatorException: Certificate has been revoked
```

Workaround On the client system, disable the Java configuration parameters from Java control panel do the following:

Step 1 Go to **Advanced > Security > General**

Step 2 Check certificates for revocation using CRL

Step 3 Enable online certificate validation

If you are using Mac, in addition to changing the Java preferences, you need to change both CRL and OCSP checking to off under **Keychain > Preferences > Certificates in OSX**.

In some scenarios, you would need to do the following if you are a Mac user:

Step 1 Go to **Keychain > Certificates.** Double-click the associated cisco.com certificate.

Step 2 Click the Trust right-arrow and select Always Trust from the When using this certificate dialog box.

Step 3 Restart the browser and connect to the CIMC web interface.(CSCtx85249)

Symptom LSI MegaRAID SAS 9240-8i is not supported in CIMC storage management.

Workaround None.(CSCtn12627)

Symptom CIMC reports loss of PSU redundancy on a one PSU system. For a system with only one PSU inserted at host on, redundancy messages should not be computed as they are not applicable.

Workaround None. (CSCtx47364)

Symptom A Cisco C210 M2 server reports a CIMC self test failed error (0x8300) in the BIOS Error Manager. This may cause the server to pause during POST if the POST Error Pause option is set in the BIOS.

Workaround This issue can be resolved by disabling hardware monitoring in ESX/ESXi.

In a local recreate, disabling the CIM agent and IPMI, then restarting CIMC, and power cycling the server resulted in the CIMC self-test not failing going forward. However, this results in ESXi and vCenter not having any hardware monitoring capability. There has been no adverse affects seen from the CIMC self test failing so the tradeoff of not seeing the CIMC self test failure error versus not having hardware monitoring capabilities in ESXi and vCenter needs to be weighed. If the CIM agent and IPMI are enabled in ESXi, the POST Error Pause option in the BIOS needs to be disabled so that the server does not pause during POST.(CSCtt34444)

KVM/vMedia

Symptom The duration counter does not start after mapping the device over vMedia.

Workaround Remove the device and reattach it or restart the client.(CSCtx02473)

BIOS

Symptom In the C200, C210 and C250 servers, the BIOS setup displays mirrored DIMMs incorrectly. The mirrored DIMMs are listed as “Installed” instead of ““Mirror Unit”.

Workaround Use the CIMC to view the DIMMs that are used as mirror units.(CSCtr77593)

Symptom When you upgrade the CIMC or BIOS from Release 1.3 to Release 1.4, the LOM ports are not detected by the operating system or the CIMC because the onboard network interface card (NIC) is disabled in the BIOS. The LOM ports displays the MAC address as 00:00:00:00:00:00.

Workaround Change the BIOS configuration as follows:

BIOS > Advanced > PCI configuration > Onboard NIC# > enabled(CSCtu40828)

Symptom As per VMware KB 1030265, UCS C-series servers running VMware ESX/ESXi 4.1 or ESXi 5.0 may experience the following symptoms:

- HBAs stop responding.
- Other PCIs devices may also stop responding.
- You see an illegal vector shortly before an HBA stops responding to the driver.

Example 1:

```
vmkernel: 6:01:34:46.970 cpu0:4120)ALERT: APIC: 1823: APICID 0x00000000 - ESR = 0x40
```

The HBA stops responding to commands.

Example 2:

```
vmkernel: 6:01:42:36.189 cpu15:4274)<6>qla2xxx 0000:1a:00.0: qla2x00_abort_isp: ****
FAILED ****
vmkernel: 6:01:47:36.383 cpu14:4274)<4>qla2xxx 0000:1a:00.0: Failed mailbox send register
test
```

The HBA card is marked as offline.

Example 3:

```
vmkernel: 6:01:47:36.383 cpu14:4274)<4>qla2xxx 0000:1a:00.0: ISP error recovery failed -
board disabled
```

As the messages log file rolls over quickly on an ESXi host, press Alt + F11 on the ESXi physical console. The following error message appears in red:

```
ALERT: APIC: 1823: APICID 0x00000000 - ESR = 0x40
```

This message is cleared out on reboot.

Workaround The workaround for this issue is listed below:

Note This issue only applies if you see this specific alert in the vmkernel/messages log files:

```
ALERT: APIC: 1823: APICID 0x00000000 - ESR = 0x40.
```

If you do not see this message, you are not experiencing this issue.

To workaround this issue, disable interrupt mapping on your ESX/ESXi 4.1 and 5.0 host and reboot the host to apply the settings.

ESX/ESXi 4.1

- To disable interrupt remapping on ESX/ESXi 4.1, perform one of these options:

  Run these commands from a console or SSH session:

  ```
  # esxcfg-advcfg -k TRUE iovDisableIR
  # reboot
  ```

- To check if interrupt mapping is set after the reboot, run the command:

  ```
  # esxcfg-advcfg -j iovDisableIR
  iovDisableIR=TRUE
  ```

- In vSphere Client, perform the following steps:

Step 1 Click Configuration > (Software) Advanced Settings > VMkernel.

Step 2 Select VMkernel.Boot.iovDisableIR and click OK.

Step 3 Reboot the ESX host.

ESXi 5.0

ESXi 5.0 does not provide this parameter as a GUI client configurable option. It can only be changed via esxcli or PowerCLI.

- To set the interrupt mapping via esxcli:

  List the present setting:

  ```
  # esxcli system settings kernel list -o iovDisableIR
  ```

  The output is similar to:

  ```
  Name          Type  Description                              Configured  Runtime
  Default
  ------------  ----  ---------------------------------------  ----------  -------
  -------
  iovDisableIR  Bool  Disable Interrrupt Routing in the IOMMU  FALSE        FALSE
  FALSE
  ```

  Disable interrupt mapping on the host with this command:

  ```
  # esxcli system settings kernel set --setting=iovDisableIR -v TRUE
  ```

  Reboot the host after running the command.

- To set the interrupt mapping through PowerCLI:

  ```
  PowerCLI> Connect-VIServer -Server 10.21.69.233 -User Administrator -Password passwd
  PowerCLI> $myesxcli = Get-EsxCli -VMHost 10.21.69.111
  PowerCLI> $myesxcli.system.settings.kernel.list("iovDisableIR")


  Configured  : FALSE
  Default     : FALSE
  Description : Disable Interrrupt Routing in the IOMMU
  Name        : iovDisableIR
  Runtime     : FALSE
  Type        : Bool


  PowerCLI> $myesxcli.system.settings.kernel.set("iovDisableIR","TRUE")
  true

  PowerCLI> $myesxcli.system.settings.kernel.list("iovDisableIR")

  Configured  : TRUE
  Default     : FALSE
  Description : Disable Interrrupt Routing in the IOMMU
  Name        : iovDisableIR
  Runtime     : FALSE
  Type        : Bool
  ```

- After the host has finished booting you see this entry in the log file /var/log/boot.gz confirming that interrupt mapping has been disabled:

```
TSC: 543432 cpu0:0)BootConfig: 419: iovDisableIR = TRUE
```

(CSCtw68712)

CLI

Symptom The following errors are observed when the CIMC is upgraded to 1.4(1a):

- CIMC becomes unresponsive.
- CIMC Web GUI displays the “Error: 2001: Service not available” error
- Details for any scope in CIMC CLI cannot be obtained

Workaround Try the following workarounds:

- Restart the CIMC
- Preform an AC power cycle
- Unplug the power supply cable and then plug it back in after one minute(CSCts42866)

Symptom The CIMC CLI should display the PID information for chassis field replaceable units (FRU).

Workaround None.(CSCtg28226)

Symptom CIMC CLI grep filter fails when using quotes to search for multiple words.

Workaround None.(CSCtw61900)

LOM

Symptom The optional 10GE LOM on C260 server does not interoperate with NX-OS 5.1 on Nexus 5000 and Nexus 2000 platforms.

Workaround None.(CSCtx13264)

Release 1.4(2)

The following caveats were fixed in 1.4(2) release

CIMC

Symptom When “ipmitool sdr” command is entered at the command prompt, an unspecified error is observed.

[root@localhost ~]# ipmitool sdr

Get SDR xxxx command failed: Unspecified error

Workaround None. (CSCtr99251)

Symptom The CIMC firmware upgrade utility can cause an error on the CIMC that will cause System Event Log (SEL) messages to be repeated as if the CIMC had just been restarted.

Workaround None. Firmware upgrade will complete successfully, but dozens of extra redundant SEL messages can occur. (CSCtl12301)

Symptom When you reboot/upgrade the CIMC firmware through the WebGUI, the WebGUI will redirect to login page. When you try to login, you will get a message “session is already active, please logout to clear the existing session”. You will get the same message, even after you logout, and login again.

Workaround You must clear the cookies/cache to login successfully. (CSCts39518)

LSI

Symptom SNMP trap is not received when check consistency has failed. This issue is seen with certain firmware releases of the LSI Storage controller.

Workaround Update the LSI storage controller firmware. (CSCtr90017)

Release 1.4(1e)

The following caveat was resolved in the 1.4(1e) release:

BIOS

Symptom Attempt to reset the C250 server from the BMC causes spurious ECC uncorrectable errors.

Workaround Do not reset the server from the BMC, instead power down and power up the server. (CSCtt35212)

Release 1.4(1)

The following caveats were resolved in the 1.4(1) release:

BIOS

Symptom If you enter into the LSI Option ROM Configuration utility WebBIOS, by pressing <CNTRL-H> during boot, the BIOS boot order changes. So after exiting the WebBIOS and rebooting, the system might not boot in the same order as expected previously.

Workaround After exiting the WebBIOS (which reboots the system anyway), update the Boot order by entering BIOS Setup. Follow these steps:

Step 1 Press F2 to enter the BIOS Setup.

Step 2 Go to **Boot Option** Tab, select "Hard Disk Order" and update the boot order as required.

Step 3 Update the Boot Option #1, #2, and so on.

Step 4 Save and exit (F10). (CSCta56788)

Symptom Some boot order configurations can not be applied as expected using only the CIMC interfaces, the server BIOS settings will have an affect that may be unexpected. If for example you specify a boot order of CDROM, HDD, and the BIOS setting is HDD, CDROM, PXE, EFI in BIOS, the applied configuration will be CDROM, HDD, PXE, EFI. Another example would be that if you do not have FDD devices and specify a boot order in CISM of FDD, CDROM, HDD, the FDD will not be appllied. The resulting configuration will be CDROM, HDD.

Workaround None. (CSCtc74741)

Symptom When VT-UTF8 is selected as a terminal type in the BIOS Setup, junk characters are seen on the terminal.

Workaround Do not select the VT-UTF8 terminal type, instead use the VT100 default mode. (CSCtb25124)

CIMC

Symptom Immediately after switching off the main CPU in C460 M1 rack server, the CIMC becomes unresponsive.

Workaround Restart the CIMC. (CSCtl56864)

Symptom On some UCS C210 servers, FAN4 and FAN5 TACH sensors are showing status as CRITICAL and the speed is 0.

Workaround None. (CSCtr11881)

Symptom BIOS configuration is not saved in CIMC exported configuration.

Workaround None. (CSCtl72671)

Symptom Gradual memory leak over a period of time is seen in CIMC, which may lead to Out of Memory (OOM) scenario. This is observed when the SNMP feature is enabled.

Workaround None. This has been resolved in 1.3(3) and 1.4(1). (CSCto53530)

Symptom Disabling SNMP feature from Cisco CLI fails.

Workaround Use WebGUI to disable SNMP feature. This is available in the page **Admin->Communications services**. (CSCtq28791)

Symptom If you enter special characters for a VNIC name like "("or")" then a core is generated.

Workaround Special characters should be assigned in quotes. For example, If assigning cd()() as the name of the VNIC, it should be enclosed in quotes in the GUI as "cd()()". (CSCto54995)

Symptom Image files created by the Virtual Media subsystem are created in the user's desktop directory.

Workaround There is no workaround. Currently image files are always created in the user's desktop directory. Once the image file is created a user can move it anywhere, but the creation process is currently in a fixed location. (CSCtk59127)

LOM

Symptom C460 10GE LOM ports are not supported in RHEL 5.6. Broadcom netxtreme2-6.0.XX Linux drivers cannot be compiled in RHEL 5.6.

Workaround Broadcom does not support RHEL5.6 in this release. (CSCtn17919)

LSI

Symptom LSI Storage controllers on C-460 M1, C200 M2, C250-M2 servers running ESX4.1 and ESXi4.1 cannot be managed using the host application MegaRAID Storage Manager running on remote clients.

Workaround The LSI controller can be managed using WebBIOS which can be accessed using Cntrl+H keys during BIOS bootup when LSI controller is scanned. (CSCtk06208)

Symptom The host based LSI tool MegaCli when executed will display a “Permission Denied” message on ESXi4.1 and ESX4.1 operating system.

Workaround After installing MegaCli on ESXi4.1 or ESX4.1, use the following command to change permission: chmod 755 MegaCli. Once the permission is changed, MegaCli command and options work successfully. (CSCtk11863)

KVM

Symptom User sees out of date (without KVM and VM tabs) KVM/vMedia client windows.

Workaround When running 1.3(1) software, if a KVM session is initiated, and the client does not have separate KVM and VM tabs, then it almost certainly indicates an older client is being run. The solution is to clear the java cache on the system. This is different than the browser cache. On Windows XP, follow these steps:

Step 1 Navigate to the **Control Panel -> Java Control Panel**.

Step 2 Click on the **Settings** button in the Temporary Internet Files panel.

Step 3 Click on the **Delete Files** button in the Temporary Files Settings popup box.

Step 4 Be sure to check the Applications and Applets checkbox and then click **OK**. (CSCtn41499)

Symptom User is not allowed to choose file name when creating vMedia image files.

Workaround The .img file created when using the vMedia “Create Image” feature is the same as the directory from which the contents are created with the “.img” extension added. Before creating the file, you can change the directory name to match what you would like the final file name to be. (CSCtk59152)

Known Behaviors

This section includes the following topics:

Release 1.4(3s)4

The following is the known behavior found in the 1.4(3s)4 release:

Symptom LSI firmware update will fail using HUU 1.4.3s.4 if the LSI controller has a version prior to 2.120.xxx.xxx on it.

Workaround Complete the following steps:

Step 1 Update LSI controller firmware using HUU 1.3.1c.

Step 2 Reboot the server

Step 3 Boot to HUU 1.4.3s.4 and update the LSI controller firmware. (CSCug39576)

Release 1.4(3j)

The following are the known behaviors found in the 1.4(3j) release:

CIMC

Symptom In C460 servers, the shared_lom_10g CIMC network mode with active-standby redundancy can stop working when the host OS is also using 10GE LOM port and is rebooted.

Workaround Do not use the CIMC network mode shared_lom_10g. Use one of the other modes instead.(CSCtj57061)

Symptom In C460 servers, the shared_lom_10g CIMC network mode with active-active redundancy can stop working when the host OS is also using 10GE LOM port.

Workaround Do not use the CIMC network mode shared_lom_10g. Use one of the other modes instead. (CSCtj58245)

Symptom The CIMC cisco_card network mode can result in a few duplicate CIMC packets in the network which can cause the ipmitool to fail and ping to report duplicate packets.

Workaround This issue will be resolved in the future versions of the ipmitool.(CSCty61805)

BIOS

Symptom While upgrading from Release 1.3(2i) to Release 1.4(3c) on C460 M1, a moderate fault is observed and you get a bad reading of "CATERR_N". The Windows 2008 R2 operating system appears frozen and pressing Ctrl+ Alt + Del does not take you to the login screen. In ESXi, you may encounter the pink screen of death (PSOD).

Workaround Check the BIOS CPU setting on CIMC by navigating to **Server** -> **BIOS**-> **Configure BIOS** -> **Advanced** and you may see the c1E state and the C state (located at the bottom of processor configuration section) in “unknown” state. Change the state to “disabled”, save the changes and reboot the server.(CSCtz31007)

Release 1.4(3)

The following are the known behaviors found in the 1.4(3) release:

CIMC'

Symptom PI2CPerformOP ioctl driver failures are displayed in the CIMC log due to the presence of 3Y PSUs.

Workaround Use Cisco PSU having the part number label as 74-7541-02.

Symptom The PSU firmware revision may only be partially available when the PSU does not have AC power.

Workaround Connect the AC power to the PSU. The full firmware revision will be available.(CSCtx43305)

Symptom C460 CIMC network mode shared_lom_10g with active-active redundancy will lose connectivity temporarily when the host OS is also using a 10GE LOM port.

Workaround Do not use CIMC network mode shared_lom_10g. Use one of the other modes instead (CSCtj58245)

LSI

Symptom In C460 server, when you use LSI 9240-8i HBA with more than 8 drives, the system hangs in BIOS POST, displays the following message and waits for user input:

```
Number of disks exceeded the maximum supported count of 8 disks. Please remove the extra
drives and reboot system to avoid losing data. Press "Y" to continue with extra drives.
```

Workaround When using LSI 9240-8i HBA in C460 server, limit the number of installed drives to a maximum of 8 drives (CSCtw59886)

Release 1.4(2)

The following are the known behaviors found in the 1.4(2) release:

BIOS

Symptom BIOS boot order configuration from CIMC or UCSM may not be successful sometimes.

Workaround After BIOS boot order configuration, restart the system. Or wait for the BIOS boot to complete before configuring the boot order. (CSCts70906)

Symptom Installation of any UEFI Aware Operating System may result in a complete system failure.

Workaround No workaround exists. We do not support UEFI aware Operating Systems. (CSCtd71780)

CIMC

Symptom Network mode cannot be set to cisco_card mode even though the option is available.

Workaround Install Cisco UCS P81E card to move into cisco_card network mode. (CSCth87044)

Misc

Symptom Cannot install VMware on ICH10 SATA controller in SW RAID mode.

Workaround None. (CSCtb49393)

Web UI

Symptom The following message appears after installation or upgrade to ESX 4.0 vSphere:
`Error:TSC: 1137350434cpu0 :0)NUMA : 827 Signficant imbalance between NUMA nodes detected. Performance may be impacted.:`

Workaround There are two possible workarounds.

Option 1: Ensure that memory configuration is equal across both processors. Ensure that there are equal amounts of DIMMs of the same size and speed inserted in the DIMM sockets.

Option 2: Reboot system and enter BIOS setup by pressing F2. Go to **Advanced-->Memory Configuration-->Memory RAS --> Performance Configuration**--> and change NUMA Optimized to Disabled. Press F10 to save and reboot. (CSCtc33846)

Symptom Windows 2008 R2 installation fails with the following message: “The Computer restarted unexpectedly or encountered an unexpected error. Windows installation cannot proceed. To install Windows, click OK to restart the computer, and then restart the installation”

Workaround Remove the Intel Quad port GbE HBA Adapter during windows install.(CSCtt01897)

Symptom BIOS

Symptom After upgrading to BIOS version 1.2.1a.0, one of the two onboard LOMs may get disabled.

Workaround After upgrading to BIOS version 1.2.1a.0, reboot the server, go to the BIOS setup screen, navigate to the **Advanced -> PCI Configuration** screen, and set the “Onboard Gbit NIC2” to enabled. Then save and exit the BIOS setup. (CSCti71226)

CIMC

Symptom The CIMC Web GUI doesn't come up after certificate import. The browser displays the following Error message: Error Invalid Server Certificate. A request failed because the server's certificate was invalid.

Workaround Provide different values for the corresponding fields for “Subject Information” and “Issuer Information” during the certificate import process. (CSCth63837)

Symptom After using the WSMAN command the session displays the following error message: Error: Unable to create Resource Locator object.

Workaround There is no workaround. This request is not valid. You will need to provide a valid target so that CIMC can return appropriate information. (CSCth43327)

Symptom Occasionally IPMI LAN interfaces will become unresponsive (to the point of lost functionality) under stress.

Workaround The workaround is not to use IPMI queries during times of high SOL traffic. (CSCtd05874)

Symptom The uboot version shows extra character after normal CIMC version.

Workaround The extra character is displayed after updating to 1.2.x revisions of the firmware. This is a new feature added to the release and it specifies a specific uboot version. (CSCti49855)

Symptom Two active media sessions observed in the webUI/CLI.

Workaround Reset to default through the webUI or CLI so that the new changes take effect. (CSCti42465)

LSI

Symptom When the installation of the LSI SNMP agent on a Windows OS is complete, an error message that reads as “Fatal Error” may be displayed, indicating an unsupported version of firmware is installed on the storage controller.

Workaround The firmware version installed on the storage controller must be a supported version. To view the list of supported firmware versions for the controller, see: http://www.cisco.com/en/US/products/ps10477/prod_technical_reference_list.html (CSCti35162)

Symptom When there are 8708 and 1064E LSI controllers on the same system, the product name of the 1064E controller is displayed as “UNUSED” on the MIB walk.

Workaround Remove the 8708 LSI controller and place only the 1064E to view the product name in the MIB walk. (CSCti64538)

Open Caveats

Release 1.4(3)

This section lists the open caveats for the 1.4(3) release:

CIMC

Symptom Using the CIMC Web GUI, you cannot use only numbers to set a Common Name (CN). For example, you cannot have 3456 as a common name.

Workaround Use the CLI.(CSCun24570)

Symptom When CIMC is booted, the HTTP Web UI does not start.

Workaround Restart the CIMC.(CSCtx19968)

Symptom 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.

Workaround Restart the CIMC.(CSCtx88183)

Symptom When hard disks are removed from RAID groups, the CIMC Web GUI and CLI may show the same drives as online in the Physical tab of the Storage page and as missing in the Virtual Drive tab.

Workaround Restart the CIMC.(CSCtx81754)

Symptom When BIOS starts, a "Error on Getting CIMC IP/MAC Address" message is displayed.

Workaround This message can be ignored.(CSCtx27907)

Symptom When LSI controller is downgraded, you may view the information, for example, virtual drive, firmware, of the previous version of the LSI controller in the CIMC Web GUI and CLI.

Workaround Restart the host machine so that the correct information is propagated to the CIMC Web GUI and CLI.(CSCtx08449)

Symptom In Release 1.4(2), when the CIMC firmware is upgraded, the storage information does not get displayed in CIMC Web GUI and CLI.

Workaround Restart the CIMC.(CSCtx08443)

Symptom The keyboard can stop working in the Broadcom 57712 PCIe option ROM.

Workaround None.(CSCtr04410)

BIOS

Symptom When you enter into the LSI 1064E option ROM, **RAID Properties** option is disabled.

Workaround Enable the option ROM for slots 6 and 7 (the mezzanine slot) in the server BIOS. (CSCub17899)

Symptom When BIOS console redirection is enabled, the keyboard can stop working in the Broadcom PCIe option ROM at some baud rates.

Workaround Disable the BIOS console redirection.(CSCtq84425)

LSI

Symptom The C460 server with 9240-8i card hangs and results in system panic or BSOD when a virtual drive is being deleted from Linux or Windows using the LSI host applications such as MegaRAID Storage Manager (MSM) or MegaCli.

Workaround Limit to one stripe size for all Virtual Drives on a controller. If you require multiple stripe sizes and encounter the VD deletion issue, restart the system and delete the VD using the Web BIOS.(CSCtx41090)

Symptom The C460 server with 9240-8i card hangs during the virtual drive creation when you use either MSM or MegaCli LSI applications from any of the supported OS.

Workaround Restart the system if the system hangs during the virtual drive creation. We recommend you limit to one stripe size for all the VDs on a controller.(CSCtw64310)

Misc

Symptom When you update the P81E VIC firmware to Release 1.6(2a), it is observed that the SAN boot installation uses the ESX 4.1.x and ESXi 5.0 but after post-install, the ESX and ESXi hosts fails to establish network connectivity either through DHCP or Static IP.

Workaround None.(CSCtx34605)

Release 1.4(2)

This section lists the open caveats for the 1.4(2) release:

BIOS

Symptom When the BIOS parameters are configured from CIMC CLI or WebUI interfaces, the configuration might not take effect.

Workaround Re-configure the BIOS parameters. (CSCtn46192)

CIMC

Symptom A Cisco C200 or C210 rack server may have a "Disturbingly high number of I2C errors" message in the systems logs; when the installed OS is ESXi 4.1 or ESXi 5.0.

Workaround None known at this time. (CSCtt70347)

Symptom CIMC power capping is not supported on VMware ESXi 5.0.

Workaround When CIMC is upgraded to 1.4(2), the CIMC will automatically disable power capping. Power capping must manually be re-enabled to use it. (CSCtt08424)

LSI

Symptom The hard disk slot numbering on C260 in the LSI Host Applications such as MSM and BMC WebUI/CLI may not match with the Physical Slot numbers on the silkscreen in the front panel of the servers. The condition occurs in C260 configurations which have 1 or 2 LSI controllers with Non-Expander Backplane. If there is one LSI controller, there will be only one enclosure and the disk numbering would be 0-7. If there are two LSI controllers, there will be two enclosures and the disk slot numbering would be 0-7 on Enclosure 1 and 0-7 on Enclosure 2.

Workaround The hard disk slots 0-7 on Enclosure 1 from Host Application MSM corresponds to 1-8 Physical HDD Slot numbers and the Hard disk slot 0-7 on Enclosure 2 from Host Application MSM corresponds to 9-16 Physical HDD Slot numbers on the Front Panel Silkscreen. (CSCtq03202)

Release 1.4(1)

This section lists the open caveats for the 1.4(1) release:

BIOS

Symptom BIOS setup parameters configuration interface from CIMC does not validate runtime parameters of the system and also it is not aware of the interdependency between them. For example,

- If the memory configuration does not support memory mirroring, then BIOS setup does not show mirroring as a setup option. However, CIMC would still show the option to set mirroring.
- When the system is equipped with a 4 core CPU, BIOS setup option to disable the cores would only show upto 4 cores. However CIMC would still show the option upto 6 cores.

- When SATA controller is disabled, BIOS setup will hide the options to set other SATA controller parameters. However CIMC would still show the other SATA controller parameters.

Workaround Even though the options are shown and can be configured from CIMC, it does not create any side-effects, nor do any harm to the system. BIOS will handle them gracefully. (CSCtl21208)

Symptom BIOS downgrade using the iFlash32 utility, from 1.4.x to the older version 1.2.x fails.

Workaround Use the startup.nsh script available in the 1.2.x container for the downgrade. This script will execute the BIOS downgrade successfully. (CSCtr93601)

CIMC

Symptom SNMPV3 traps are not receiving in Net-SNMP receiver. When V3 settings are chosen for trap delivery, the SNMP trapd CLI utility fails to receive V3 traps.

Workaround There is a possibility that the SNMP trap utility might not work for V3 authentication/privilege settings. (CSCtr83298)

Symptom The AES encryption field does not show the encryption level (128/256/ etc) on the Web UI and CLI.

Workaround The SNMP V3 encryption key length must be clearly indicated. The SNMP agent supports AES - 128 bit encryption by default. (CSCtr31577)

Symptom SNMP V1 test traps are sent even when V2 or V3 traps are enabled.

Workaround There is no provision for V2 and V3 test traps in the present implementation of the SNMP agent. (CSCtr37876)

Misc

Symptom Ports on the N2XX-ABPCI02 do not come up after a reboot or power cycle when running Linux.

Workaround Power cycle the server. (CSCtk66778)

LOM

Symptom Broadcom adapters and LOMs based on BCM5709, BCM57711 and BCM57712 configured for iSCSI and FCoE boot, iSCSI and FCoE boot configuration is lost after firmware upgrade. This is observed in the following cases:

- Using a Broadcom adapter based on BCM5709, BCM57711 or BCM57712.
- Having either iSCSI boot or FCoE boot configuration in the option ROM.
- Upgrading the firmware with HUU.

Workaround Record the configuration before the firmware upgrade and reapply it after the upgrade. (CSCtr85387)

Release 1.3(2d)

This section lists the open caveats for the 1.3(2d) release:

CIMC

Symptom 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.

Workaround Connect all cables from APC power to the power supply securely. (CSCtg92856)

Symptom CIMC Web GUI and CLI correctly reports the number of failed DIMMs, but does not display which of the DIMMs have failed.

Workaround BIOS Setup (F2) or CIMC System Event Log can display the exact failed DIMMs. (CSCto09153)

Symptom On C460 servers, the CIMC Web GUI does not display Cisco P81E card details when the main CPU is powered off.

Workaround Use the CIMC CLI or power on the main CPU. (CSCtn75815)

Note Release 1.3(1) does not support UCS integration. Customers who want to integrate their C-Series server with a UCS instance must use release 1.2(x). If your server is currently running 1.3(1), you need to downgrade it using the 1.2.2 Host Upgrade Utility. For more information, see the Hardware Installation Guide for the type of server you are integrating.

Release 1.3(1c)

This section lists the open caveats for the 1.3(1c) release:

CIMC

Symptom CIMC storage view of LSI 9260 card occasionally reports 0 Cache Memory size.

Workaround There is no workaround for CIMC storage management views. You can use host-based MSM tools to corroborate data. (CSCtn08982)

Symptom When NIC mode is in shared_lom and the boot order is such that EFI is not the first one in the order and there is no other media to boot from, the following message is displayed - “Select proper media else press a key”. If you enter a key, the KVM session terminates.

Workaround Ensure that you have the proper media in place before trying to boot from the device. If not, when prompted with above message, you will have to place the required media and then reboot the host. Else have the system in dedicated mode. (CSCtl82492)

MISC

Symptom SMASH memory enumeration can fail on UCS-C460-M1.

Workaround None for SMASH interfaces. Memory related data can be retrieved through CiIC CLI or WebUI. (CSCtn29771)

vKVM/vMedia

Symptom KVM fails to launch with a pop-up “Unable to launch Application”.

Workaround Follow these steps:

Step 1 Update the JRE to http://www.java.com/en/download/inc/windows_upgrade_ie.jsp

Step 2 Close all browsers.

Step 3 Clear the cache (I**nternet Options -> Tools**).

Open a new browser window and start a CIMC session. KVM should now be able to launch. (CSCtl70994)

Symptom Garbled WebUI output when LSI 9280-4i4e card is installed and external JBOD connected.

Workaround There is no actual data integrity problem, but the displays can be significantly garbled. One workaround is to only use external or only internal on any given controller card. Another is to use host based tools to display information on controllers where both internal and external storage is connected. (CSCtn03816)

Release 1.2(2d)

This section lists the open caveats for the 1.2(2d) release:

CIMC

Symptom LED sensor color is displayed as Red or Amber or Blue (or any supported color) even though LED state if OFF.

Workaround Ignore LED color when LED state is OFF. (CSCth84883)

Symptom If you try to move to cisco_card mode from the CIMC Configuration Utility, you see the error "Net mode invalid".

Workaround Install either just one or two R2X0-PSU2-650-SB power supply units in the server. Restart the CIMC and move to cisco_card mode. (CSCti70359)

Release 1.2(1a)

This section lists the open caveats in the 1.2(1a) release:

CIMC

Symptom When updating CIMC firmware through TFTP, if the image file is corrupted, the update status indicator is the same as if the file does not exist.

Workaround Be aware that this error message can actually indicate either of the above conditions and should make sure that the file both the exists, and is a valid firmware image for the CIMC being upgraded. (CSCti17492)

BIOS

Symptom 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.

Workaround Set the new networking mode, save, then set the new IP address and save again. (CSCth71350)

Release 1.1.(2)

This section lists the open caveats for the 1.1(2a) release and applies to the M1 version of the C460 server.

MISC

Symptom 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.

Workaround None. The system boots from MegaRAID Virtual Drives only if the number of Virtual Drives are lesser than or equal to 49. (CSCtg25373)

This section lists the known behaviors for the 1.1(2a) release and applies to the M1 version of the C460 server.

BIOS

Symptom Serial port B cannot be enabled for console redirection in the Server Management —> Console Redirection page of the BIOS setup.

Workaround 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. (CSCtf54851)

Symptom System reboots during EFI Windows 2008 R2 installation.

Workaround EFI OS installation is not supported by the BIOS. You should disable the EFI- Optimized mode in the BIOS setup and install Windows 2008 R2 in legacy mode. (CSCtf87728)

Web UI

Symptom On completion of the "Recover Corrupt BIOS" wizard, clicking on the "Finish" button brings up a dialog with the message "BIOS recovery may not be in a state in which it can be canceled. Attempt to cancel anyway?"

Workaround The message is shown erroneously. Simply click "Yes" to close the message dialog. (CSCtd84141)

Symptom A name without domain part used during login in a scenario where authentication fails over from AD to CIMC does not succeed.

Workaround To connect to an AD server you need to use the full form of a user name (like bob@domain.com, even if domain.com had been specified in AD configuration). If this fails because the AD server is unreachable then login with the partial name. (CSCtd74258)

Release 1.0(1)

The following caveats were opened in UCS software release 1.0(1).

This section lists the open caveats for this release. Unless otherwise noted, the caveats are for all rack server platforms.

KVM

Symptom Launching the KVM console with Microsoft Internet Explorer browsers fails and causes the message “Internet Explorer was not able to open this Internet site. The requested site is either unavailable or cannot be found”. This error occurs with Microsoft Internet Explorer browsers with the advanced “Do not save encrypted pages to disk” option set.

Workaround From the Internet Explorer toolbar, select **Tools -> Internet Options**. The Internet Options dialog will pop up. Click the Advanced tab and uncheck the “Do not save encrypted pages to disk” option. (CSCtd19439)

Web UI

Symptom Printing from Web UI will work from Internet Explorer, but not Firefox.

Workaround None. (CSCtc22985)

Documentation Updates

Active Directory

In the section titled “Active Directory” in the Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Release 1.2(1), and the Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide, Release 1.2(1), the following statement is incorrect:

“When Active Directory is enabled in the CIMC, all user authentication and role authorization is performed by Active Directory, and the CIMC ignores the local database. If the CIMC cannot connect to Active Directory, it reverts to the local database.”

The correct behavior is as follows:

“When Active Directory is enabled, user authentication and role authorization are performed by Active Directory for user accounts not found in the local user database.”

Symptom Linux mouse emulation is calculated, unlike Windows mouse emulation. There are situations when the KVM Linux mouse emulation gets out of sync with the host's mouse: Novell/SUSE's install DVD for SLES doesn't include mouse acceleration. The X setup for the install DVD is very basic, unlike RHEL's. A mouse will work on SLES once it is installed but lags during the installation.On Linux, you

can switch between graphical and text mod using the Ctrl-Alt-F1 for text and Ctrl-Alt-F7 to go back to graphical mode. The KVM Linux mouse emulation sometimes gets out of sync when switching between modes.

Workaround When the mouse gets out of sync in Linux, the user must force KVM to recalculate it. There are two ways to force KVM to recalculate the Linux mouse: 1) In KVM, go to the **Tools->Session Options->Mouse** tab and press the button for Linux Mouse Acceleration and then press "Apply" and "OK". If the Linux Mouse Acceleration is already selected, the user can still press "Apply" and then "OK" to force it to recalculate. 2) Move the mouse out of the KVM window to the right of the window and back into the KVM window, forcing it to recalculate the mouse position again. (CSCtc12265)

Related Documentation

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

- Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Release 1.1(1)
- Cisco UCS C-Series Servers Integrated Management Controller Configuration Guide, Release 1.1(1)
- Cisco UCS C-Series Servers Integrated Management Controller CLI Command Reference, Release 1.1(1)

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*

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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

Release Notes for Cisco UCS C-Series Software, Release 1.4(3)