Release Notes for Cisco UCS Manager, Release 2.2

First Published: 2013-12-12

Last Modified: 2020-12-20

Overview

This document describes system requirements, new features, resolved caveats, known caveats and workarounds for Cisco UCS Manager software Release 2.2. This document also includes the following:

- Current information that became available after the technical documentation was published
    - Related firmware and BIOS on blade and rack servers and other Cisco Unified Computing System (UCS) components associated with the release

Use this release note as a supplement with the other documents listed in documentation roadmaps:

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

Contents of the various bundles for this release are described in:

- Release Bundle Contents for Cisco UCS Software, Release 2.2

Make sure to review other available documentation on Cisco.com to obtain current information on Cisco UCS Manager.

Support for Web User Interface Post Deprecation of Adobe Flash

The Web user interface of Cisco UCS Manager releases earlier than 3.1(3a) — including the releases on the 2.2 release train — are Java-based and may not be accessible on browser versions that will deprecate support for Adobe Flash on Dec 31, 2020. For more details on the problem description and workarounds, refer to the Field Notice: FN72012.

Revision History

Table 1: Online Change History

Date	Description
December 12, 2013	Created release notes for Cisco UCS Manager, Release 2.2(1b).

December 20, 2013	Added additional caveats.
February 9, 2014	Updated release notes for Cisco UCS Software Release 2.2(1c).
February 19, 2014	Updated release notes for Catalog Release 2.2.1c.T.
April 2, 2014	Updated release notes for Catalog Release 2.2.1d.T.
April 10, 2014	Updated release notes for Cisco UCS Software Release 2.2(1d).
May 16, 2014	Added CSCuo78883 to Open Caveats for release 2.2(1d).
May 22, 2014	Updated release notes for Cisco UCS Software Release 2.2(2c).
May 24, 2014	Updated to include additional Open Caveats for Cisco UCS Software Release 2.2(2c).
May 30, 2014	Modified several Caveat descriptions.
June 18, 2014	Added CSCul74278 to 2.2(1b) Open Caveats and to 2.2(2c) Resolved Caveats; added ‘Behavior Changes’ section; and corrected three items in Servers list.
August 1, 2014	Updated release notes for Cisco UCS Software Release 2.2(1e).
August 21, 2014	Added B22 PID support and updated PID support for other servers in Version Mapping table for 2.2(2c); added ‘Chassis’ section to Internal Dependencies table; added UCSB-5108-AC2, -DC2, and -HVDC to New Hardware Features section; added note to Upgrade section for CSCud81176 consideration; added CSCuj81245 to 2.2(1b) Open Caveats table and to 2.2(2c) Resolved Caveats table.
September 8, 2014	Updated release notes for Cisco UCS Software Release 2.2(3a).
September 11, 2014	Updated release notes for Cisco UCS Software Release 2.2(2d); updated the Recommended Minimum Software in Table 4.
October 9, 2014	Updated release notes for Cisco UCS Software Release 2.2(3b).
October 24, 2014	Updated release notes for Cisco UCS Software Release 2.2(2e) and 2.2(3c).
October 31, 2014	Updated release notes for Cisco UCS Software Release 2.2(1f).
November 10, 2014	Added CSCuo60330 to 2.2(3a) resolved caveats.
November 17, 2014	Added missing 2.2(3c) adapter to Internal Dependencies table.
December 4, 2014	Updated release notes for Catalog Release 2.2.3b.T.
December 22, 2014	Updated release notes for Cisco UCS Software Release 2.2(1g) and 2.2(3d).
January 13, 2015	Updated first affected bundle for CSCuq20755.
March 4, 2015	Updated release notes for Cisco UCS Software Release 2.2(3e).

March 18, 2015	Updated the New Hardware Features list for Release 2.2(3a).
March 20, 2015	Updated release notes for Cisco UCS Software Release 2.2(3f).
April 15, 2015	Updated the Recommended Software Version for C260 and C460 M2 servers.
May 14, 2015	Updated release notes for Cisco UCS Software Releases 2.2(3g) and 2.2(4b).
May 26, 2015	Added CSCus10255 to the Resolved Caveats for Cisco UCS Software Release 2.2(4b).
June 5, 2015	Updated release notes for Cisco UCS Software Release 2.2(5a).
June 15, 2015	Updated release notes for Cisco UCS Software Release 2.2(1h).
June 30, 2015	Updated the Capability Catalog and New Hardware Features sections with information about Cisco 12G SAS Modular RAID Controller. Updated the Resolved Caveats for 2.2(4b).
July 10, 2015	Added CSCuv04436 to the Open Caveats for 2.2(4b) and 2.2(5a). This issue has a software advisory associated with it.
July 17, 2015	Updated release notes for Cisco UCS Software Release 2.2(4c).
July 30, 2015	Updated release notes for Cisco UCS Software Release 2.2(5b).
August 27, 2015	Updated release notes for Cisco UCS Software Release 2.2(5c).
September 11, 2015	Updated the Behavior Changes section for Release 2.2(4b). Updated the Resolved and Open Caveats for Release 2.2(5c). Added CSCus81832 to the list of Resolved Caveats for Release 2.2(4b).
September 22, 2015	Added CSCus73196 to the list of Open Caveats for Release 2.2(3d).
September 25, 2015	Updated release notes for Cisco UCS Software Release 2.2(3h).
October 8, 2015	Updated release notes for Cisco UCS Software Release 2.2(6c).
October 17, 2015	Added CSCuv45173 to the Known Limitations table. This issue has a software advisory associated with it.
November 4, 2015	Updated release notes for Cisco UCS Software Release 2.2(6d).
November 16, 2015	Updated release notes for Cisco UCS Software Release 2.2(5d).
December 14, 2015	Updated release notes for Cisco UCS Catalog Release 2.2.6e.T.
December 16, 2015	Updated release notes for Cisco UCS Software Release 2.2(6e).
January 18, 2016	Updated the Behavior Changes section for Release 2.2(6c).
February 2, 2016	Updated release notes for Cisco UCS Software Release 2.2(6f).

February 9, 2016	Updated release notes for Cisco UCS Software Release 2.2(3j).
February 29, 2016	Updated release notes for Cisco UCS Software Release 2.2(6g).
March 31, 2016	Updated release notes for Cisco UCS Software Release 2.2(7b).
April 18, 2016	Updated the New Software Features description for Release 2.2(7b).
May 13, 2016	Updated release notes for Cisco UCS Software Release 2.2(3k).
May 18, 2016	Updated release notes for Cisco UCS Software Release 2.2(6i).
May 24, 2016	Added CSCuz74973 to the Open Caveats for Cisco UCS Software Release 2.2(3b), and updated the workaround for CSCut63966.
June 2, 2016	Updated release notes for Cisco UCS Software Release 2.2(7c).
June 13, 2016	Updated the note in Updating Cisco UCS Release.
June 17, 2016	Added CSCut46044 and CSCup58725 to the Open Caveats for Cisco UCS Software Release 2.2(3a). Added CSCuj84274 to the Open Caveats for Cisco UCS Software Release 2.2(1a). Added CSCut46044 to the Security Fixes for Cisco UCS Software Release 2.2(7b).
June 20, 2016	Removed note for UCS-ML-1X324RU-G and UCS-ML-1X644RU-G. Added a note for UCS-ML-1X324RV-A and UCS-ML-1X644RV-A.
July 5, 2016	Updated release notes for Cisco UCS Software Release 2.2(6j).
July 13, 2016	Updated release notes for Cisco UCS Software Release 2.2(8a). Updated the Recommended Software Version for C200, C210, and C250 M2 servers.
July 29, 2016	Updated release notes for Cisco UCS Software Release 2.2(7d).
August 8, 2016	Updated the New Software Features description for Release 2.2(7b).
August 12, 2016	Added CSCva87230 to the list of open caveats for release 2.2(8a).
August 24, 2016	Updated release notes for Cisco UCS Software Release 2.2(8b). Added software advisory associated with CSCva87230.
August 26, 2016	Updated release notes for Cisco UCS Software Release 2.2(7e).
September 29, 2016	Updated release notes for Cisco UCS Software Release 2.2(8c).
October 18, 2016	Updated release notes for Cisco UCS Software Release 2.2(8d).
November 21, 2016	Added CSCuz74973 to the Resolved Caveats for Cisco UCS Software Release 2.2(7b).
November 23, 2016	Updated release notes for Cisco UCS Software Release 2.2(8e)T.

December 22, 2016	Updated release notes for Cisco UCS Software Release 2.2(8f).
January 30, 2017	Updated release notes for Cisco UCS Software Release 2.2(3l).
March 14, 2017	Updated release notes for Cisco UCS Software Release 2.2(8g).
September 12, 2017	Updated the list of security fixes with CSCvf35705.
November 21, 2017	Updated release notes for Cisco UCS Software Release 2.2(8i).
December 15, 2017	Updated the Resolved Caveat version for CSCuu33864.
January 9, 2018	Updated the list of security fixes with CSCuq77241.
April 06, 2018	Updated release notes for Cisco UCS Software Release 2.2(8j).
May 18, 2018	Updated the Resolved Caveats for Cisco UCS Software Release 2.2(7b) with CSCun07367.
May 28, 2018	Updated the Open Caveats for Cisco UCS Software Release 2.2(1b) with CSCvj59299, CSCvj59301, CSCvj54880, CSCvj54847, CSCvj54187, and their Software Advisory.
August 01, 2018	Updated release notes for Cisco UCS Software Release 2.2(8l).
August 27, 2018	Added the L1 Terminal Fault caveats — CSCvm02934, CSCvm03356, CSCvm03351, and CSCvm03339 — to the list of Security Fixes for Cisco UCS Software Release 2.2(8l).
February 26, 2019	Added CSCvf32853 to the list of Open Caveats for Cisco UCS Software Release 2.2(8a).
October 18, 2019	Updated release notes for Cisco UCS Software Release 2.2(8m).
December 20, 2020	Added notice: Support for Web User Interface Post Deprecation of Adobe Flash.

Introduction

Cisco UCS Manager™ provides unified, embedded management of all software and hardware components of the Cisco Unified Computing System™ (Cisco UCS) across multiple chassis, rack servers, and thousands of virtual machines. Cisco UCS Manager manages Cisco UCS as a single entity through an intuitive GUI, a command-line interface (CLI), or an XML API for comprehensive access to all Cisco UCS Manager functions.

System Requirements

To use Cisco UCS Manager your computer must meet or exceed the following minimum system requirements:

- The Cisco UCS Manager GUI is a Java-based application which requires Java Runtime Environment 1.6 or later.
- Cisco UCS Manager uses web start and supports the following web browsers:

  - Microsoft Internet Explorer 9.0 or higher
  - Mozilla Firefox 7.0 or higher
  - Google Chrome 14.0 or higher

- Adobe Flash Player 10 or higher is required for some features
- Cisco UCS Manager is supported on the following operating systems:
  - Microsoft Windows 7 with minimum 4.0 GB memory
  - Red Hat Enterprise Linux 5.0 or higher with minimum 4.0 GB memory
- Cisco UCS Central integration:
  - Cisco UCS Manager Release 2.2(1) and 2.2(2) can only be registered with Cisco UCS Central, Release 1.1(1b) or higher.
  - Cisco UCS Manager Release 2.2(3) and later releases can only be registered with Cisco UCS Central, Release 1.2(1a) or higher.
  - Cisco UCS Manager Release 2.2(7) and later releases require Cisco UCS Central, Release 1.4(1b) or higher.

Note For more information, see the Feature Support Matrix section of the Cisco UCS Central Installation and Upgrade Guides.

Updating Cisco UCS Releases

The Cisco UCS Manager A bundle software (Cisco UCS Manager, Cisco NX-OS, IOM firmware) can be mixed with previous B or C bundle releases on the servers (host firmware (FW), BIOS, CIMC, adapter FW and drivers).

The following table lists the mixed A, B, and C bundle versions that are supported:

Table 2: Mixed Cisco UCS Releases Supported

	Infrastructure Versions (A Bundles)															
Host FW Versions (B or C Bundles)	**2.0(1)**	**2.0(2)**	**2.0(3)**	**2.0(4)**	**2.0(5)**	**2.1(1)**	**2.1(2)**	**2.1(3)**	**2.2(1)**	**2.2(2)**	**2.2(3)**	**2.2(4)**	**2.2(5)**	**2.2(6)**	**2.2(7)**	**2.2(8)**
2.0(1)	Yes	—	—	—	—	Yes	Yes	Yes	—	—	—	—	—	—		
2.0(2)	—	Yes	—	—	—	Yes	Yes	Yes	—	—	—	—	—	—		
2.0(3)	—	—	Yes	—	—	Yes	Yes	Yes	—	—	—	—	—	—		

	Infrastructure Versions (A Bundles)															
Host FW Versions (B or C Bundles)	**2.0(1)**	**2.0(2)**	**2.0(3)**	**2.0(4)**	**2.0(5)**	**2.1(1)**	**2.1(2)**	**2.1(3)**	**2.2(1)**	**2.2(2)**	**2.2(3)**	**2.2(4)**	**2.2(5)**	**2.2(6)**	**2.2(7)**	**2.2(8)**
2.0(4)	—	—	—	Yes	—	Yes	Yes	Yes	—	—	—	—	—	—		
2.0(5)	—	—	—	—	Yes	Yes	Yes	Yes	—	—	—	—	—	—		
2.1(1)	—	—	—	—	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.1(2)	—	—	—	—	—	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.1(3)	—	—	—	—	—	—	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.2(1)	—	—	—	—	—	—	—	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.2(2)	—	—	—	—	—	—	—	—	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.2(3)	—	—	—	—	—	—	—	—	—	—	Yes	Yes	Yes	Yes	Yes	Yes
2.2(4)	—	—	—	—	—	—	—	—	—	—	—	Yes	Yes	Yes	Yes	Yes
2.2(5)	—	—	—	—	—	—	—	—	—	—	—	Yes	Yes[1]	Yes[1]	Yes[1]	Yes[1]
2.2(6)	—	—	—	—	—	—	—	—	—	—	—	Yes[1]	Yes[1]	Yes[1]	Yes[1]	Yes[1]
2.2(7)	—	—	—	—	—	—	—	—	—	—	—	Yes[1]	Yes[1]	Yes[1]	Yes[1]	Yes[1]
2.2(8)												Yes[1]	Yes[1]	Yes[1]	Yes[1]	Yes[1]

[1] Beginning with Cisco UCS Manager Release 2.2(4), and for M4 servers, a lower version of the infrastructure A bundle will be compatible with the previous version and higher version of B and C server bundles. For example, the Cisco UCS Manager Release 2.2(4)A bundle will be supported with any of the following B bundles for B200-M4 servers: 2.1(1)B, 2.1(2)B, 2.1(3)B, 2.2(1)B, 2.2(2)B, 2.2(3)B, 2.2(4)B, 2.2(5)B, 2.2(6)B, 2.2(7)B, 2.2(8)B.

Note For M1, M2, M3 servers, only N, N-1 cross-version firmware is supported. For example, for B200 M3 servers, the 2.2(4)A bundle will be supported with 2.1(1)B, 2.1(2)B, 2.1(3)B, 2.2(1)B, 2.2(2)B, 2.2(3)B, and 2.2(4)B bundles).

- If upgrading from a pre-2.2(1b) release and running Management Firmware Pack, refer to open caveat information for CSCud81176 in Release Notes for Cisco UCS Software, Release 2.1.
- If an environment includes a mix of servers, refer to CSCuh61202 and CSCus64439 for caveat information.

Note To avoid this issue, first upgrade any Cisco UCS 1240, Cisco UCS 1280, and Cisco M81KR adapter firmware before updating the Cisco UCS infrastructure components—Cisco UCS Manager, IOM, and FI.

- During manual or auto firmware installs, the fabric interconnect may fail to reload after a reboot or power cycle. Refer to CSCut63966 for caveat information.

  A workaround for this issue is to modify a script file, which is called before any reboots occur. This modification can limit the chances of experiencing this issue during an upgrade to firmware versions in which this issue is resolved. Contact Cisco TAC for more information regarding this workaround, and to recover from this issue.

- A mix of servers running different B-bundles may be run with a single A-bundle. However, any given server must be running the entire B/C-bundles (with associated drivers). Example: mixing the 2.1(2)B BIOS with the 2.1(3)B CIMC on a server is not supported.

- The OS hardware and software interoperability is relative to the B/C-bundle on any given server. To see what OS is supported, see the Hardware and Software Interoperability documentation associated with the B-bundle version.

- For all M3 or older servers released with Cisco UCS Manager Release 2.2(3) and earlier versions, the A-bundle version must be at or above the same version(s) of any B/C-bundles running on the servers (see Table 2). This applies to patch levels as well, even though they are not displayed on the table. For example, you can mix 2.1(1f)A with 2.1(1b)B, but you cannot mix 2.1(1b)A with 2.1(1f)B.

  You do not need the A-bundle version to be at or above the same version(s) of any B/C-bundles when using Cisco UCS Manager Release 2.2(4) and later releases with M4 servers.

  For all M1, M2, M3, and M4 servers released with Cisco UCS Manager Release 2.2(4) and later versions, the patch version of the A-bundle version does not affect the compatibility with B/C bundles running on the servers. The patch versions within a release, such as 2.2(8a) and 2.2(8e), are always supported regardless of the combination. For example, you can mix 2.2(4b)A with 2.2(4c)B, or 2.2(4c)A with 2.2(4b)C.

- Some features introduced in Cisco UCS Release 2.2 require that both the A-bundle version and the B/C-bundle versions be upgraded to the same version. For example, the lower power budget supported for Cisco UCS Release 2.2 is not supported for servers using 2.1 firmware.

- In Cisco UCSM Release 2.2 and later releases, the adapter firmware version is different from the Cisco UCSM Release version.

Minimum B/C Bundle Version Requirements for Cisco UCS Manager Features

The following Cisco UCS Manager 2.2 features require the specified minimum B/C bundle version to perform expected operations:

Table 3:

Feature	B Bundle Version	C Bundle Version
IPv6 Management Support	2.2(1b)B	2.2(1b)C
usNIC for Low Latency	2.2(1b)B	2.2(1b)C

Feature	B Bundle Version	C Bundle Version
Support for Virtual Machine Queue (VMQ)	2.2(1b)B	2.2(1b)C
VM-FEX for Hyper-V Management with Microsoft SCVMM	2.2(1b)B	2.2(1b)C
Secure Boot	2.2(1b)B	2.2(1b)C
Local Storage Management	2.2(1b)B	2.2(1b)C
Flash Adapters and HDD Firmware Management	2.2(1b)B	2.2(1b)C
Precision Boot Order Control	2.2(1b)B	2.2(1b)C
Trusted Platform Module (TPM) Inventory	2.2(1b)B	2.2(1b)C
DIMM Blacklisting and Correctable Error Reporting	2.2(1b)B	2.2(3a)C
Netflow monitoring support: • Cisco UCS VIC 1240 and 1280 • Cisco UCS VIC 1225 • Cisco UCS VIC 1227 • Cisco UCS VIC 1340 and 1380 • Cisco UCS VIC 1225T and 1227T	2.2(2c)B — — 2.2(3a)B —	— 2.2(2c)C 2.2(3a)C — 2.2(4b)C
Stateless Offload for Overlay Networks (NVGRE / VXLAN) **Note** Supported only on Cisco UCS VIC 1340 and VIC 1380 adapters.	2.2(3a)B	—
BIOS secure boot support	2.2(1b)B	2.2(3a)C
CIMC secure boot support	2.2(1b)B	2.2(3a)C

Feature	B Bundle Version	C Bundle Version
RDMA over Converged Ethernet (RoCE) support for Microsoft SMB Direct **Note** Supported only on Cisco UCS VIC 1340 and VIC 1380 adapters.	2.2(4b)B	—
LLDP support for Fabric Interconnect vEthernet Interfaces	2.2(4b)B	2.2(4b)C
Policy-based port error handling	2.2(4b)B	2.2(4b)C
Advanced Local Storage Configuration	2.2(4b)B	2.2(4b)C
Pass-through capability for Gen 3 Fusion IO Mezzanine cards	2.2(4b)B	—
Fabric Interconnect traffic evacuation	2.2(4b)B	2.2(4b)C
Per Fabric Interconnect chassis reacknowledgment	2.2(4b)B	—
Trusted Platform Module (TPM) configuration support	2.2(4b)B	2.2(4b)C
Consistent Device Naming (CDN) support **Note** CDN is supported only on Windows 2012 R2.	2.2(4b)B	2.2(4b)C
CIFS authentication protocol support for Scriptable vMedia	2.2(4b)B	2.2(4b)C
Support for Service Profile migration with UEFI boot mode	2.2(4b)B	2.2(4b)C
Support NVGRE with IPv6 and VMQ	2.2(4b)B	—
Support usNIC with Intel® MPI	2.2(4b)B	2.2(4b)C
Server support for 4K Drives	—	2.2(4b)C

For detailed instructions for updating the Cisco UCS software and firmware, see the appropriate Upgrading Cisco UCS document for your installation.

Hardware and Software Interoperability

For a complete list of hardware and software interdependencies, see the *Hardware and Software Interoperability for UCSM Managed Servers* for a specific Cisco UCS Manager release, here:

http://www.cisco.com/c/en/us/support/servers-unified-computing/unified-computing-system/products-technical-reference-list.html

Internal Dependencies

The table shows interdependencies between the hardware and versions of Cisco UCS Manager. Server FRU items such as DIMMs are dependent on their server type, and chassis items such as fans and power supplies work with all versions of Cisco UCS Manager.

Table 4: Internal Dependencies

Component	Minimum Qualified Software Version[1]	Recommended Software Version
Servers		

B22 M3 E5-2400
B22 M3 E5-2400 v2
	2.1(3k)
	2.2(2e)
		2.2(8m)
		2.2(8m)

B200 M1 and M2	2.2(2e)	2.2(8m)

B200 M3 E5-2600
B200 M3 E5-2600 v2
	2.1(3k)
	2.2(2e)
		2.2(8m)

B200 M4 E5-2600 v3 B200 M4 E5-2600 v4[2]	2.2(3a)	2.2(8m)
	2.2(7b)	2.2(8m)
B230 M1 and M2	2.1(3k)	2.2(8m)
B250 M1 and M2	2.1(3k)	2.2(8m)

B260 M4 E7-2800 v2
B260 M4 E7-4800 v2
B260 M4 E7-8800 v2
B260 M4 E7-4800 v3
B260 M4 E7-8800 v3
B260 M4 E7-4800 v4
B260 M4 E7-8800 v4
	2.2(2e)
	2.2(2e)
	2.2(2e)
	2.2(5d)
	2.2(5d)
	2.2(8c)
	2.2(8c)
		2.2(8m)
		2.2(8m)
		2.2(8m)
		2.2(8m)
		2.2(8m)
		2.2(8m)
		2.2(8m)

B420 M3 E5-4600
B420 M3 E5-4600 v2
	2.1(3k)
	2.2(2e)
		2.2(8m)
		2.2(8m)

B440 M1 and M2	2.1(3k)	2.2(8m)

Component	Minimum Qualified Software Version[1]	Recommended Software Version
Servers		
B420 M4 E5-4600 v3	2.2(5d)	2.2(8m)
B420 M4 E5-4600 v4	2.2(8a)	2.2(8m)
B460 M4 E7-4800 v2	2.2(2e)	2.2(8m)
B460 M4 E7-8800 v2	2.2(2e)	2.2(8m)
B460 M4 E7-4800 v3	2.2(5d)	2.2(8m)
B460 M4 E7-8800 v3	2.2(5d)	2.2(8m)
B460 M4 E7-4800 v4	2.2(8c)	2.2(8m)
B460 M4 E7-8800 v4	2.2(8c)	2.2(8m)
C22 M3 and M3L	2.1(3k)	2.2(8m)
C24 M3, M3L, and M3S2	2.1(3k)	2.2(8m)
C200 M2 and M2 SFF	2.1(3k)	2.2(8m)
C210 M2	2.1(3k)	2.2(8m)
C220 M3[3]	2.1(3k)	2.2(8m)
C220 M4	2.2(3k)	2.2(8m)
C220 M4 E5-2600 v4	2.2(7c)	2.2(8m)
C240 M3[3]	2.1(3k)	2.2(8m)
C240 M4	2.2(3k)	2.2(8m)
C240 M4 E5-2600 v4	2.2(7c)	2.2(8m)
C250 M2	2.1(3k)	2.2(8m)
C260 M2	2.1(3k)	2.2(8m)
C420 M3	2.1(3k)	2.2(8m)
C460 M2	2.1(3k)	2.2(8m)
C460 M4 E7-2800 v2	2.2(2e)	2.2(8m)
C460 M4 E7-4800 v2	2.2(2e)	2.2(8m)
C460 M4 E7-8800 v2	2.2(2e)	2.2(8m)
C460 M4 E7-4800 v3	2.2(5d)	2.2(8m)
C460 M4 E7-8800 v3	2.2(5d)	2.2(8m)
C460 M4 E7-8800 v4	2.2(8d)	2.2(8m)

Component	Minimum Qualified Software Version[1]	Recommended Software Version
Servers		
Adapters		
UCS 82598KR-CI UCS M71KR-E UCS M71KR-Q	2.1(3k)	2.2(8m)
UCS M81KR	2.1(3k)	2.2(8m)
UCS NIC M51KR-B UCS CNA M61KR-I[4] UCS CNA M72KR-Q UCS CNA M73KR-Q UCS CNA M72KR-E	2.1(3k)	2.2(8m)
UCS-VIC-M82-8P UCSB-MLOM-40G-01 UCSB-MLOM-PT-01	2.1(3k)	2.2(8m)
UCSB-MLOM-40G-03 UCSB-VIC-M83-8P UCSC-MLOM-CSC-02	2.2(3a)	2.2(8m)
UCSB-MEZ-ELX-03 UCSB-MEZ-QLG-03 UCSC-PCIE-CSC-02	2.1(3k)	2.2(8m)
UCSC-F-FIO-1000MP UCSC-F-FIO-1300MP UCSC-F-FIO-2600MP UCSC-F-FIO-5200MP	2.2(3a)	2.2(8m)
UCSB-FIO-1600MS UCSB-FIO-1300MS	2.2(3a)	2.2(8m)
UCSC-INVADER-3108 UCSC-NYTRO-200GB	2.2(3a)	2.2(8m)

Component	Minimum Qualified Software Version[1]	Recommended Software Version
Servers		
UCSC-MLOM-C10T-02 UCSC-PCIE-C10T-02 UCSC-F-FIO-785M UCSC-F-FIO-365M UCSC-F-FIO-1205M UCSC-F-FIO-3000M UCSC-F-FIO1000PS UCSC-F-FIO1300PS UCSC-F-FIO2600PS UCSC-F-FIO5200PS UCSC-F-FIO-6400SS UCSC-F-FIO-3200SS	2.2(4b)	2.2(8m)
GPU		
UCSB-GPU-M6	2.2(7b)	2.2(8m)
Chassis[5]		
N20-C6508	2.2(1b)	2.2(8m)
UCSB-5108-DC	2.2(1b)	2.2(8m)
UCSB-5108-AC2	2.2(1b)	2.2(8m)
UCSB-5108-DC2	2.2(1b)	2.2(8m)
UCSB-5108-HVDC	2.2(2c)	2.2(8m)
Fabric Interconnect		
UCS 6120XP	2.2(7c)	2.2(8m)
UCS 6140XP	2.2(7c)	2.2(8m)
UCS 6248UP	2.2(7c)	2.2(8m)
UCS 6296UP	2.2(7c)	2.2(8m)
Fabric Extender or I/OM		
UCS 2104	2.2(7c)	2.2(8m)
UCS 2208XP	2.2(7c)	2.2(8m)

Component	Minimum Qualified Software Version[1]	Recommended Software Version
Servers		
UCS 2204XP	2.2(7c)	2.2(8m)
Cisco Nexus 2232PP	2.2(7c)	2.2(8m)
Cisco Nexus 2232TM-E	2.2(7c)	2.2(8m)
Fabric Interconnect Expansion Modules		
N10-E0440 N10-E0600 N10-E0080	**2.2(7c)**	2.2(8m)
N10-E0060	2.2(7c)	2.2(8m)
UCS-FI-E16UP	2.2(7c)	2.2(8m)
Power Supplies		
UCSC-PSUV2-1050DC	2.2(7c)	2.2(8m)
UCSB-PSU-2500HVDC	2.2(7c)	2.2(8m)
UCSC-PSU-930WDC UCSC-PSU1-770W UCSC-PSU2-1400 UCSC-PSU2V2-650W UCSC-PSU2V2-1200W	2.2(7c)	2.2(8m)
NVME SSD Drives		
UCS-SDHPCIE800GB	2.2(7c)	2.2(8m)
UCS-SDHPCIE1600GB[1]	2.2(7c)	2.2(8m)
10-GB Connections		
SFP-10G-SR, SFP-10G-LR SFP-H10GB-CU1M SFP-H10GB-CU3M SFP-H10GB-CU5M	2.2(7c)	2.2(8m)
SFP-H10GB-ACU7M SFP-H10GB-ACU10M	2.2(7c)	2.2(8m)

Component	Minimum Qualified Software Version[1]	Recommended Software Version
Servers		
FET-10G SFP-10G-AOC[7]: SFP-10G-AOC1M SFP-10G-AOC2M SFP-10G-AOC3M SFP-10G-AOC5M SFP-10G-AOC7M SFP-10G-AOC10M	2.2(7c)	2.2(8m)
8-GB Connections (FC Expansion Module N10-E0060)		
DS-SFP-FC8G-SW DS-SFP-FC8G-L	2.2(7c)	2.2(8m)
4-GB Connections (FC Expansion Module N10-E0080)		
DS-SFP-FC4G-SW DS-SFP-FC4G-LW	2.2(7c)	2.2(8m)
1-GB Connections		
GLC-T (V03 or higher) GLC-SX-MM GLC-LH-SM	2.2(7c)	2.2(8m)

1. This is the minimum server bundle recommended for this hardware in a mixed firmware configuration, assuming the infrastructure is at the recommended software version.

2. Cisco UCS Manager Release 2.2(4) introduced a server pack feature that allows Intel E5-2600 v4 CPUs to run with Cisco UCS Manager Release 2.2(4) or later releases, provided the CIMC, BIOS, and Capability Catalog are all running Cisco UCS Manager Release 2.2(7). For upgrading B200 M4 servers from v3 CPUs to v4 CPUs, refer to Cisco UCS B200 M4 Server Upgrade Guide for E5-2600 v4 Series CPUs.

3. See the Software Advisory for the minimum firmware level required on the Cisco UCS C220 M3 and Cisco UCS C240 M3.

4. N20-AI0002, the Cisco UCS 82598KR-CI 10-Gb Ethernet Adapter, is not supported on the B440 server but is still available for other models. We suggest you use the Cisco UCS CNA M61KR-I Intel Converged Network Adapter in place of the Cisco UCS 82598KR-CI 10-Gb Ethernet Adapter.

5. Recommended minimum software versions do not take into account mixed environments; to determine the minimum software version for your mixed environment, refer to, Updating Cisco UCS Releases, on page 6.

6. For 1.6 TB HGST NVME drives, when used with B200-M4 blade servers, the minimum required board controller version is 12, which is bundled with Cisco UCS Manager Release 2.2(7c)B.
7. Cisco 1225 and 1227 VIC cards are not supported with SFP-10G-AOC cables. SFP-10G-AOC cables are only supported with Cisco 1385 and 1387 VIC cards.

Capability Catalog

The Cisco UCS Manager uses the catalog to update the display and configurability of server components such as newly qualified DIMMs and disk drives. The Cisco UCS Manager Capability Catalog is a single image, but it is also embedded in Cisco UCS Manager. Cisco UCS Manager 2.2(x) releases work with any 2.2(x) catalog file, but not the 1.x, 2.0 or 2.1 catalog versions. If a server component is not dependent on a specific BIOS version, using it and having it recognized by Cisco UCS Manager is primarily a function of the catalog version. The catalog is released as a single image in some cases for convenience purposes in addition to being bundled with UCS infrastructure releases. See Table 5 for details on the mapping of versions to bundles.

Table 5: Version Mapping

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
2.2(8m)	ucs-catalog.2.2.8k.T.bin	—	—
2.2(8l)	ucs-catalog.2.2.8k.T.bin	—	—

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
2.2(8j)	ucs-catalog.2.2.8k.T.bin		—

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
		Drives • UCS-SD960GIKS4-EV • UCS-SD120GBMS4-EV • UCS-SD240GBMS4-EV • UCS-SD480GBMS4-EV • UCS-SD960GBMS4-EV • UCS-SD16TBMS4-EV • UCS-SD19TBMS4-EV • UCS-SD38TBMS4-EV • UCS-SD76TBMS4-EV • UCS-SD240GBM1K9 • UCS-SD960GBM1K9 • UCS-SD38TBM1K9 • UCS-S3260-HD8TB • UCS-S3260-8TBRR • UCS-HD1T7KL6GA • UCS-HD4T7KL6GA • UCS-HD6T7KL6GA • UCS-SD480GSAS-EV • UCS-SD960GSAS-EV • UCS-SD19TSAS-EV • UCS-SD38TSAS-EV • UCS-SD400GSAS3-EP • UCS-SD800GSAS3-EP • UCS-SD16TSASS3-EP • UCS-SD32TSASS3-EP • UCS-HD2T7KL6GA **Note** Orderable with hardware and software RAID	

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
		configuration.	
2.2(8g)	ucs-catalog.2.2.8h.T.bin	--	--
2.2(8f)	ucs-catalog.2.2.8f.T.bin	**Cisco UCS C220, C240, B200, B420, and S3260 CPUs** UCS-CPU-E52699AE	--
--	ucs-catalog.2.2.8e.T.bin	**Drives** UCS-SD480GBKS-EV UCS-SD19TBKSS-EV	--
2.2(8d)	ucs-catalog.2.2.8d.T.bin	--	--
2.2(8c)	ucs-catalog.2.2.8c.T.bin	--	--
2.2(8b)	ucs-catalog.2.2.8b.T.bin	--	--

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
2.2(8a)	ucs-catalog.2.2.8a.T.bin		**CPU** • UCS-CPU-E5-4660D • UCS-CPU-E5-4650D • UCS-CPU-E5-4640D • UCS-CPU-E5-4620D • UCS-CPU-E5-4610D • UCS-CPU-E5-4669D • UCS-CPU-E5-4667D • UCS-CPU-E5-4655D • UCS-CPU-E5-4627D **Memory** • UCS-MR-1X081RU-A • UCS-MR-1X162RU-A • UCS-MR-1X161RV-A • UCS-ML-1X324RV-A • UCS-MR-1X322RV-A • UCS-MR-2X082RY-E • UCS-MR-2X162RY-E • UCS-ML-2X324RY-E • UCS-ML-2X648RY-E • UCS-MR-1X081RU-G • UCS-MR-1X162RU-G • UCS-MR-1X322RU-G

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
		Cisco UCS B420 M4 **CPU** • UCS-CPU-E5-4660E • UCS-CPU-E5-4650E • UCS-CPU-E5-4640E • UCS-CPU-E5-4620E • UCS-CPU-E5-4610E • UCS-CPU-E5-4669E • UCS-CPU-E5-4667E • UCS-CPU-E5-4655E • UCS-CPU-E5-4627E **Memory** • UCS-MR-1X322RV-A • UCS-MR-1X161RV-A • UCS-ML-1X324RV-A • UCS-ML-1X644RV-A **TPM** • UCSX-TPM2-002 **C460 M4 E7-8800 v4** **CPU** • UCS-CPU-E78890E • UCS-CPU-E78880E • UCS-CPU-E78870E • UCS-CPU-E78860E • UCS-CPU-E74850E • UCS-CPU-E74830E • UCS-CPU-E74820E • UCS-CPU-E74809E • UCS-CPU-E78891E • UCS-CPU-E78893E	

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
		• UCS-CPU-E78867E **Memory** • UCS-MR-1X161RV-G **TPM** • UCSX-TPM1-002 **B260 M4 and B460 M4 E7- 4800 v4 , E7-8800 v4** **CPU** • UCS-CPU-E78890E • UCS-CPU-E78880E • UCS-CPU-E78870E • UCS-CPU-E78860E • UCS-CPU-E74850E • UCS-CPU-E74830E • UCS-CPU-E74820E • UCS-CPU-E74809E • UCS-CPU-E78891E • UCS-CPU-E78893E • UCS-CPU-E78867E **Memory** • UCS-MR-1X161RV-G • UCS-MR-1X322RU-G • UCS-ML-1X644RU-G • UCS-ML-1X324RU-G **HDD** • UCS-SD120GB7M-EV • UCS-SD16TB7M-EV • UCS-SD480GB7M-EP **TPM** • UCSX-TPM1-002	

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
2.2(7e)	ucs-catalog.2.2.7c.T.bin	—	—
2.2(7d)	ucs-catalog.2.2.7c.T.bin	—	—
2.2(7c)	ucs-catalog.2.2.7c.T.bin	—	—

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
2.2(7b)	ucs-catalog.2.2.7b.T.bin		**Memory** • UCS-ML-1X324RU-A • UCS-MR-1X081RU-G • UCS-MR-1X162RU-A • UCS-MR-1X162RU-G • UCS-MR-1X322RU-G • UCS-MR-2X162RY-E

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
		Cisco UCS B200 M4, C220 M4, and C240 M4 CPUs • UCS-CPU-E52699E • UCS-CPU-E52698E • UCS-CPU-E52697AE • UCS-CPU-E52697E • UCS-CPU-E52695E • UCS-CPU-E52690E • UCS-CPU-E52683E • UCS-CPU-E52680E • UCS-CPU-E52667E • UCS-CPU-E52660E • UCS-CPU-E52658E • UCS-CPU-E52650E • UCS-CPU-E52650LE • UCS-CPU-E52643E • UCS-CPU-E52640E • UCS-CPU-E52637E • UCS-CPU-E52630E • UCS-CPU-E52630LE • UCS-CPU-E52623E • UCS-CPU-E52620E • UCS-CPU-E52609E **Storage Controller** • UCSB-LSTOR-PT **PCIe adapter card** • UCSC-SAS12GHBA **Memory** • UCS-ML-1X324RU-G	

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
		- UCS-ML-1X644RU-G - UCS-MR-1X081RV-A - UCS-MR-1X161RV-A - UCS-MR-1X322RV-A - UCS-ML-1X324RV-A **Note** Requires Cisco UCS Manager Release 2.2(7c) or later releases. - UCS-ML-1X644RV-A **Note** Requires Cisco UCS Manager Release 2.2(7c) or later releases. **Drives** - UCS-SD400GBK9 - UCS-HD1T7KL12G - UCS-HD2T7KL12G - UCS-HD4T7KL12G - UCS-HD2T7KL6GA - UCS-HD10T7KL4K - UCS-HD4TBK9 - A03-D300GA2 - A03-D600GA2 - UCS-HDD900GI2F106 - UCS-SD16TBKS4-EV **GPU**	

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
		• UCSB-GPU-M6 **Note** UCSB-GPU-M6 Requires Cisco UCS Manager 2.2(7b) or later releases. • UCSC-GPU-M60 **Crypto Card** • CSB-MEZ-INT8955 **NVME Drives** • UCS-SDHPCIE800GB • UCS-SDHPCIE1600GB **Note** For 1.6 TB HGST NVME drives, when used with B200-M4 blade servers, the minimum required board controller version is 12, which is bundled with Cisco UCS Manager Release 2.2(7b)B. **Qlogic network adapters** • UCSC-PCIE-QNICBT • UCSC-PCIE-QNICSFP **Cisco UCS VIC adapters** • UCSC-PCIE-C40Q-03 • UCSC-MLOM-C40Q-03	
2.2(6j)	—	—	—
2.2(6i)	—	—	—

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
2.2(6g)	—	—	—
2.2(6f)	ucs-catalog.2.2.6f.T.bin	—	—
2.2(6e)	—	—	—
—	ucs-catalog.2.2.6e.T.bin	—	• UCS-SD480GBKS4-EV • UCS-SD16TBKS4-EV • UCS-HD600G10KS4K • UCS-MR-2X162RY-E • UCS-SD480G12S3-EP • UCS-SD120GBKS4-EV • UCS-SD16TB12S3-EP
2.2(6d)	—	—	

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
2.2(6c)	ucs-catalog.2.2.6c.T.bin		

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
		Additional Memory • UCS-ML-1X324RU-A • UCS-ML-1X324RU-G • UCS-ML-1X648RU-G • UCS-MR-1X162RY-A • UCS-MR-2X162RX-C • UCS-MR-2X162RY-E **Drives** • UCS-HD12TB10K12G • UCS-HD1T7K12G • UCS-HD1T7K6GA • UCS-HD2T7K12G • UCS-HD2T7KL12G • UCS-HD300G10K12G • UCS-HD300G15K12G • UCS-HD450G15K12G • UCS-HD4T7KL12G • UCS-HD600G10K12G • UCS-HD600G15K12G • UCS-HD8T7KL4K • UCS-HD900G10K12G • UCS-SD16TB12S3-EP • UCS-SD16TB12S4-EP • UCS-SD16TBKS4-EV • UCS-SD240GBKS4-EV • UCS-SD38TBKS4-EV • UCS-SD400G12S4-EP • UCS-SD480G12S3-EP • UCS-SD480GBKS4-EV • UCS-SD800G12S4-EP	

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
		• UCS-SD960GBKS4-EV	
2.2(5d)	—	—	
2.2(5c)	ucs-catalog.2.2.5b.T.bin	—	
2.2(5b)	—	**Cisco UCS B420 M4 (UCSB-B420-M4)** • Memory: UCS-MR-1X648RU-A	

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
2.2(5a)	ucs-catalog.2.2.5a.T.bin		

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
		Cisco UCS B420 M4 (UCSB-B420-M4) **CPU** • UCS-CPU-E5-4660D • UCS-CPU-E5-4650D • UCS-CPU-E5-4640D • UCS-CPU-E5-4620D • UCS-CPU-E5-4610D • UCS-CPU-E5-4669D • UCS-CPU-E5-4667D • UCS-CPU-E5-4655D • UCS-CPU-E5-4627D **Memory** • UCS-MR-1X322RU-A • UCS-MR-1X162RU-A • UCS-MR-1X081RU-A **Cisco UCS B260 M4 (UCSB-B260-M4) and Cisco UCS B460 M4 (UCSB-B460-M4)** **CPU** • UCS-CPU-E78890D • UCS-CPU-E78880D • UCS-CPU-E78870D • UCS-CPU-E78860D • UCS-CPU-E74850D • UCS-CPU-E74830D • UCS-CPU-E74820D • UCS-CPU-E74809D • UCS-CPU-E78891D • UCS-CPU-E78893D	

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
		• UCS-CPU-E78880LD • UCS-CPU-E78867D **Memory** • UCS-MR-2X082RY-E • UCS-MR-2X162RY-E • UCS-ML-2X324RY-E • UCS-ML-2X648RY-E **Cisco UCS C460 M4 (UCSC-C460-M4)** **CPU** • UCS-CPU-E74809D • UCS-CPU-E74820D • UCS-CPU-E74830D • UCS-CPU-E74850D • UCS-CPU-E78860D • UCS-CPU-E78867D • UCS-CPU-E78870D • UCS-CPU-E78880D • UCS-CPU-E78880LD • UCS-CPU-E78890D • UCS-CPU-E78891D • UCS-CPU-E78893D **Memory** • UCSC-MRBD2-12 • UCS-MR-1X081RU-G • UCS-MR-1X162RU-G • UCS-MR-1X322RU-G **Storage Controller** • UCSC-MRAIDC460 • UCSC-MRAID12G	

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
		GPU • UCSC-GPU-K80	
2.2(4c)	—	**Additional Cisco UCS B200 M4** • UCS-MR-1X648RU-A	
2.2(4b)	ucs-catalog.2.2.4b.T.bin[1]	**Additional Cisco UCS B200 M4, C220 M4, and C240 M4 Memory** • UCS-MR-1X322RU-A **Additional Cisco UCS C220 M4, and C240 M4 Memory** • UCS-MR-1X648RU-A **Adapters** • UCSC-MLOM-C10T-02 • UCSC-PCIE-C10T-02 • UCSC-PCIE-Q8362 **Drives** • UCS-HD18TB10KS4K • UCS-HD600G10KS4K **Fabric Extender** • N2K-C2232TM-E-10GE	
2.2(3l)	—	—	—
2.2(3k)	—	—	—
2.2(3j)	—	—	—
2.2(3h)	ucs-catalog.2.2.3d.T.bin	—	
2.2(3g)	ucs-catalog.2.2.3c.T.bin	—	
2.2(3f)	—	—	
2.2(3e)	—	—	
2.2(3d)	—	—	

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
—	ucs-catalog.2.2.3b.T.bin1	—	
2.2(3c)	—	**Additional Cisco UCS B200 M4 CPUs** • UCS-CPU-E52640D • UCS-CPU-E52630D • UCS-CPU-E52630LD • UCS-CPU-E52623D • UCS-CPU-E52620D • UCS-CPU-E52609D • UCS-CPU-E52637D • UCS-CPU-E52650LD	
2.2(3b)	—	—	

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
2.2(3a)	ucs-catalog.2.2.3a.T.bin[1]		

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
		Cisco UCS B200 M4 (UCSB-B200-M4) **CPU** • UCS-CPU-E52699D • UCS-CPU-E52698D • UCS-CPU-E52697D • UCS-CPU-E52695D • UCS-CPU-E52690D • UCS-CPU-E52683D • UCS-CPU-E52680D • UCS-CPU-E52670D • UCS-CPU-E52667D • UCS-CPU-E52660D • UCS-CPU-E52658D • UCS-CPU-E52650D • UCS-CPU-E52643D **Memory** • UCS-MR-1X081RU-A • UCS-MR-1X162RU-A • UCS-ML-1X324RU-A **Fusion IO Memory** • UCSB-F-FIO-1300MP • UCSB-F-FIO-1600MS **Cisco UCS C220 M4 (UCSC-C220-M4) and Cisco UCS C240 M4 (UCSC-C240-M4)** **CPU** • UCS-CPU-E5-2620 • UCS-CPU-E5-2630 • UCS-CPU-E5-2630L	

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
		• UCS-CPU-E5-2640 • UCS-CPU-E5-2643 • UCS-CPU-E5-2650 • UCS-CPU-E5-2650L • UCS-CPU-E5-2660 • UCS-CPU-E5-2665 • UCS-CPU-E5-2670 • UCS-CPU-E5-2680 • UCS-CPU-E5-2690 **Memory** • UCS-MR-1X081RU-A • UCS-MR-1X162RU-A • UCS-ML-1X324RU-A	
2.2(2e)	—	—	
2.2(2d)	—	—	

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
2.2(2c)	ucs-catalog.2.2.2c.T.bin[1]		

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
		Cisco UCS B22 M3 (UCSB-B22-M3) **CPU** • UCS-CPU-E52470B • UCS-CPU-E52450B • UCS-CPU-E52440B • UCS-CPU-E52430LB • UCS-CPU-E52403B • UCS-CPU-E52420B • UCS-CPU-E52407B **Memory** • UCS-ML-1X324RY-A • UCS-MR-1X162RY-A • UCS-MR-1X082RY-A • UCS-MR-1X041RY-A **Cisco UCS B260-M4 (UCSB-EX-M4-1)** **CPU** • UCS-CPU-E78893B • UCS-CPU-E78891B • UCS-CPU-E78880LB • UCS-CPU-E78857B • UCS-CPU-E74890B • UCS-CPU-E74880B • UCS-CPU-E74870B • UCS-CPU-E74860B • UCS-CPU-E74850B • UCS-CPU-E74830B • UCS-CPU-E74820B • UCS-CPU-E74809B • UCS-CPU-E72890B	

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
		• UCS-CPU-E72880B • UCS-CPU-E72870B • UCS-CPU-E772850B **Memory** • UCS-ML-2X324RY-E • UCS-MR-2X162RY-E • UCS-MR-2X082RY-E **Cisco UCS B420-M3 (UCSB-B420-M3)** **CPU** • UCS-CPU-E54603B • UCS-CPU-E54627B • UCS-CPU-E54610B • UCS-CPU-E54650B • UCS-CPU-E54607B • UCS-CPU-E54620B • UCS-CPU-E54640B • UCS-CPU-E54657LB **Memory** • UCS-ML-1X324RZ-A • UCS-MR-1X162RZ-A • UCS-MR-1X082RZ-A **Cisco UCS B460-M4 (UCSB-EX-M4-1)** **CPU**	

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
		- UCS-CPU-E74809B - UCS-CPU-E74820B - UCS-CPU-E74830B - UCS-CPU-E74850B - UCS-CPU-E74860B - UCS-CPU-E74870B - UCS-CPU-E74880B - UCS-CPU-E74890B - UCS-CPU-E78857B - UCS-CPU-E78880LB - UCS-CPU-E78891B - UCS-CPU-E78893B **Memory** - UCS-ML-2X324RY-E - UCS-MR-2X082RY-E - UCS-MR-2X162RY-E	
2.2(1h)	—	—	
2.2(1g)	—	—	
2.2(1f)	—	—	
2.2(1e)	ucs-catalog.2.2.1d.T.bin	—	
2.2(1d)	ucs-catalog.2.2.1d.T.bin[1]	—	
—	ucs-catalog.2.2.1d.T.bin[1]	UCS-HD12T10KS2-E UCS-ML-1X324RY-A UCS-MR-2X041RY-B UCS-MR-2X082RY-B	

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
—	ucs-catalog.2.2.1c.T.bin[1]	UCS-MR-1X041RY-A UCS-MR-1X082RY-A UCS-MR-1X082RZ-A UCS-MR-2X041RX-C UCS-MR-2X082RX-C UCS-MR-2X162RX-C	
2.2(1c)	ucs-catalog.2.2.1b.T.bin	—	
2.2(1b)	ucs-catalog.2.2.1b.T.bin	UCS-ML-1X324RZ-A UCS-SD200G0KS2-EP UCS-SD400G0KS2-EP UCS-SD800G0KS2-EP UCSB-5108-AC2 UCSB-5108-DC2	

[1] Available for separate download.

Further details are in the Cisco UCS Manager Configuration Guides.

New Hardware Features in Release 2.2

New Hardware Features in Release 2.2(8m)

None

New Hardware Features in Release 2.2(8l)

None

New Hardware Features in Release 2.2(8j)

None

Release 2.2(8f) adds support for the following:

- Cisco C220, C240, B200, B420, and S3260 shipping with Intel® Xeon® Processor E5 2699A v4 series CPU

Release 2.2(8c) adds support for the following:

- Cisco UCS B260 and B460 M4 shipping with Intel® Xeon® Processor E7-4800 v4 and E7-8800 v4 series CPUs

- Cisco UCS C460 M4 shipping with Intel® Xeon® Processor E7-8800 v4 series CPUs

Release 2.2(8a) adds support for the following:

- Cisco UCS B420 M4 shipping with Intel® Xeon® Processor E5-4600 v4 series CPUs
- Trusted Platform Module (TPM) 2.0 for B260, B420, B460 and C460 M4 servers

Release 2.2(7b) adds support for the following:

- Cisco UCS B200 M4, C220 M4, and C240 M4 shipping with the Intel® Xeon® Processor E5-2600 v4 series CPUs on Cisco UCS 6100 and 6200 Series fabric interconnects
- NVIDIA Tesla M6 GPU accelerator for B200 M4 servers
- NVIDIA Tesla M60 GPU accelerator for C-Series Servers
- UCSB-LSTOR-PT storage controller
- SX350 Fusion IO adapters:
    - UCSC-F-S32002
    - UCSC-F-S13002
    - UCSC-F-S16002
    - UCSC-F-S64002
- UCSC-SAS12GHBA PCIe adapter card
- UCS-RAID9286CV-8E RAID controller
- UCSC-C240-M4SNEBS
- PCIe SSD on B200 M4 servers
- Trusted Platform Module (TPM) 2.0
- QLogic QLE8442 10Gb Dual port 10GBaseT network adapter
- QLogic QLE8442 10Gb Dual port SFP+ network adapter
- Cisco UCS VIC 1385 and VIC 1387 network adapters
- Emulex OCE14102 B network adapter

Release 2.2(5a) adds support for the following:

- Cisco UCS B420 M4 servers shipping with Intel E5-4600 v3 series CPUs
- Cisco UCS B260 M4 and B460 M4 servers shipping with Intel E7-4800 v3 series or E7-8800 v3 series CPUs
- Cisco UCS C460 M4 servers shipping with Intel E7-4800 v3 series and E7-8800 v3 series CPUs
- Cisco 12G SAS Modular RAID Controller (12-port)

- Cisco 12G SAS Modular RAID Controller support for Cisco UCS C460 M4 servers
- NVIDIA Tesla K80 GPU accelerator for C-Series servers

Release 2.2(4b) adds support for the following:

- Cisco UCS VIC 1227T adapter modular LOM (mLOM) for Cisco UCS C220 M4 and C240 M4 servers
- Cisco UCS VIC 1225T adapter for C-Series servers[1]
- Cisco UCS VIC 1340 and VIC 1380 adapters for Cisco UCS B420 M3 server[2]
- Cisco UCSC-PCIE-Q8362 adapter for all M3 and M4 C-Series servers
- Cisco Nexus 2232TM-E 10GE Fabric Extender with support for Cisco UCS VIC 1225T and VIC 1227T adapters.

[1] Except for Cisco UCS C22 M3, C24 M3 and C420 M3 servers

[2] Cisco UCS VIC 1340 and VIC 1380 adapters only support Cisco 6200 Series Fabric Interconnects and later models.

Release 2.2(3a) adds support for the following:

- Cisco UCS B200 M4 servers shipping with Intel E5-2600 v3 series CPUs
- Cisco UCS C220 M4/C240 M4 servers shipping with Intel E5-2600 v3 Series CPUs
- Cisco UCS VIC 1227 adapter modular LOM (mLOM) for Cisco UCS C220 M4 and C240M4 servers
- Cisco UCS VIC 1340 and VIC 1380 adapters for Cisco UCS B200 M3, B200 M4, B260 M4, and B460 M4 servers2
- Fusion IO ioMemory for B-series and C-series servers
- LSI Nytro MegaRaid NMR 8110-4i for C240 M3 server
- NVIDIA Tesla K40 GPU accelerator for C-Series Servers
- Emulex OCE14102 CNA
- FX3S Support
- 10GB TwinAx cables (2m)
- 10GB AOC cables (1m, 2m, 3m, 5, 7m, and 10m)

Release 2.2(2c) adds support for the following:

- B22 M3 servers shipping with Intel E5-2400 v2 CPUs.
- B420 M3 servers shipping with Intel E5-4600 v2 CPUs.
- B260 M4 servers shipping with two Intel E7-2800 v2 or E7-4800 v2 or E7-8800 v2 CPUs.
- B460 M4 servers shipping with four Intel E7-4800 v2 or E7-8800 v2 CPUs.
- C22 M3/C24 M3 servers shipping with Intel E5-2400 v2 CPUs.

- C460 M4 servers shipping with two or four Intel E7-4800 v2 or E7-8800 v2 CPUs.
- Chassis with updated backplane and High Voltage DC support (200v DC - 380v DC) - UCSB-5108-HVDC

Release 2.2(1b) adds support for the following:

- Chassis with updated backplane UCSB-5108-AC2 or UCSB-5108-DC2

New Software Features in Release 2.2

New Software Features in Release 2.2(8m)

None

New Software Features in Release 2.2(8l)

None

New Software Features in Release 2.2(8j)

None

Release 2.2(8a) adds support for the following:

- **Next Boot**—The maintenance policy now provides an **On Next Boot** option. This option is used in combination with either **User Ack** or **Timer Automatic**. With the On Next Boot option enabled, one of the following conditions can trigger the associated FSM to apply the changes waiting for the **User Ack**, or the **Timer Automatic** maintenance window.
    - If the host OS reboots, shuts down, or resets, initiated from an external, non-UCS source
    - If the server resets, or shuts down
- **Graceful shutdown**—When you acknowledge a server reboot using the graceful shut down options or a change in the service profile that requires the server reboot, Cisco UCS Manager waits until the time specified time in the maintenance policy before performing a hard shut down.
- **Health monitoring of end points**—Enhanced health monitoring of end points for fabric interconnects, IOMs, FEXes, blade servers, and rack servers.
- **Power synchronization between servers and their associated service profiles**—Cisco UCS Manager includes a global (default) power sync policy to synchronize the power state between the associated service profiles and the servers when the desired power state of the service profile differs from the actual power state of the server. The power sync policy applies to all the service profiles by default. You can edit the default policy, but cannot delete it. You can also create your own policies and apply them to service profiles.
- **Factory reset of blade servers**—You can now reset a blade server to its factory settings. By default, the factory reset operation does not affect storage drives and flexflash drives. This is to prevent any loss of data. However, you can also choose to reset these devices to a known state.
- **Support for 160 LDAP group maps**—Cisco UCS Manager now supports a maximum of 160 LDAP group maps.

- **Virtual Volume Support**—Virtual volume support is now supported for ESXi 5.5 and higher.

Release 2.2(7b) adds support for the following:

- **Firmware Upgrade Checks the VIF/Interface Status After Fabric Interconnect Reboot**—During firmware upgrade, to ensure proper functioning of all services on the fabric interconnect, it is essential to ensure that port configurations and services that go down when the fabric interconnect reboots are re-established after the fabric interconnect comes back up. Cisco UCS Manager displays any service that is not re-established after the last reboot of a fabric interconnect.
- **vNIC Redundancy Pair**— Supports two vNICs/vHBAs that are being configured with a common set of parameters through the vNIC/vHBA template pair. This prevents the configuration between two vNICs/vHBAs from going out of sync. Multiple vNIC/vHBA pairs can be created from the same vNIC/vHBA template pair.
- Ability to perform UCS Manager initial configuration without console connectivity based on DHCP lease availability.
- Preserving the following properties during backup or import operations:
  - User-defined labels for Chassis, FEX, Rack Servers, IOMs and Blade Servers
  - Assigned IDs for Chassis, FEX and Rack Servers
- **Locator LED support for server hard-disks**—You can now identify where a specific disk is inserted in a blade or rack server using the local locator LED.
- When you add new servers or adapters to an existing Cisco UCS system with a Cisco UCS Manager release that does not support these servers and adapters, discovery of the system may fail. In case of such a failure, the FSM will display an error message that the server or adapter is not supported on the current UCS firmware version. To resolve this issue, do one of the following:
  - Update the Capability Catalog to the latest compatible release
  - Upgrade the Cisco UCS Manager infrastructure firmware to the version required by the new hardware.
- **Provision to Reset Peer I/O Modules to Factory Defaults**—Sometimes, I/O module upgrades can result in failures or I/O modules can become unreachable from Cisco UCS Manager due to memory leaks. You can now reboot an I/O module that is unreachable through its peer I/O module.

  Resetting the I/O module restores the I/O module to factory default settings, deletes all cache files and temporary files, but retains the size-limited OBFL file.
- **vNIC template CDN Source**—Enables you to select the Consistent Naming Device (CDN) Source as the vNIC Name, which in turn can either be customized or derived from the vNIC instance.
- **NVMe PCIe SSD Inventory**—Cisco UCS Manager discovers, identifies, and displays the inventory of Non-Volatile Memory Express (NVMe) Peripheral Component Interconnect Express (PCIe) SSD storage devices. You can view the health of the storage devices in the server. NVMe with PCIe SSD storage devices reduce latency, increase input/output operations per second (IOPS), and lower power consumption compared to SAS or SATA SSDs.
- **PCH SSD Controller Definition**—Cisco UCS Manager Platform Controller Hub (PCH) Solid State Drive (SSD) Controller Definition provides a local storage configuration in storage profiles where you can configure all the disks in a single RAID or in a JBOD disk array.

- **Host Firmware Package Enhancement**—You can now exclude firmware of specific components from a host firmware package either when creating a new host firmware package or when modifying an existing host firmware package. For example, if you do not want to upgrade RAID controller firmware through the host firmware package, you can exclude RAID controller firmware from the list of firmware package components.

  Local disk firmware is excluded from the host firmware package by default.

- **Installed Firmware Tab Enhancement**—The Installed Firmware tab now displays all the firmware available on the blade server, including SAS controller firmware, FlexFlash controller firmware, and Disk firmware.
- **Provision to suppress VIF down alert**—When a blade server that is associated with a service profile is shut down, the VIF down alert F0283 and F0479 are automatically suppressed.
- **EFI Shell as a Boot Device**—You can create a boot policy with an EFI Shell as the boot device. Booting from an EFI Shell prevents loss of data and provides more options to script, debug, and control various booting scenarios. EFI Shell is supported as a boot device only in the Uefi boot mode.
- **Multicast Hardware Hash**—In a port channel, by default, ingress multicast traffic on any port in the fabric interconnect (FI) selects a particular link between the IOM and the fabric interconnect to egress the traffic. To reduce potential issues with the bandwidth, and to provide effective load balancing of the ingress multicast traffic, hardware hashing is used for multicast traffic. When multicast hardware hashing is enabled, all links between the IOM and the fabric interconnect in a port channel can be used for multicast traffic.
- **Reset All Memory Errors**—Provides the ability to clear all the errors from the UCS Manager.
- **CPLD Update of the UCSB-MRAID12G Storage Controller**—Starting with Cisco UCS Manager Release 2.2(7b), the infrastructure bundle now supports a CPLD component update. The CPLD update for the UCSB-MRAID12G storage controller can be triggered by doing one of the following:
  - Re-acknowledging the server—If the server did not go through a deep-assoc after upgrading to the Cisco UCS Manager 2.2(7) or later releases.
  - Updating the associated HFP with a supported B bundle—If the server was associated after upgrading to the Cisco UCS Manager 2.2(7) or later releases.
- **VM-FEX Support**—Support for ESX VM-FEX added. The support matrix in the Hardware and Software Interoperability Matrix for this release provides more details.
- **SHA-2 Certificate Support**—Support for SHA-2 certificate added.

Release 2.2(6c) adds support for the following:

- **KVM**—The Virtual Media > Activate Virtual Devices is available.

Release 2.2(4b) adds support for the following:

- **Server Pack**—This feature allows you to support new server platforms* on existing infrastructure without requiring a complete firmware upgrade. In this model, new B/C server bundles enabling the new servers will be supported on the previous infrastructure A bundle. For example, Release 2.2(5) B/C server bundles are supported with Release 2.2(4) infrastructure A bundle as highlighted in Updating Cisco UCS Releases, on page 6. New features introduced in the B/C bundles may only become available after upgrading the A bundle to the respective version.

The Server Pack feature provides the additional flexibility of adding new server platforms to active UCS domains without incurring the operational overhead of upgrading firmware across the whole domain.

*The feature will apply to select server platforms.

- **RDMA over Converged Ethernet (RoCE) for Microsoft SMB Direct**—RoCE is a link layer protocol, and hence, it enables communication between any two hosts in the same Ethernet broadcast domain. RoCE delivers superior performance compared to traditional network socket implementations because of lower latency, lower CPU utilization and higher utilization of network bandwidth.

  RoCE for Microsoft SMB Direct is supported only on Windows 2012 R2 with Cisco UCS VIC 1340 and 1380 adapters.

- **LLDP Support for Fabric Interconnect vEthernet Interfaces**—You can enable and disable LLDP on a vEthernet interface and retrieve information about LAN uplink neighbors. When using Cisco UCS with Cisco Application Centric Infrastructure (ACI), LAN uplinks of the Fabric Interconnect are connected to ACI leaf nodes. Enabling LLDP on a vEthernet interface will help the Application Policy Infrastructure Controller (APIC) to identify the servers connected to the Fabric Interconnect by using vCenter.

- **Policy-Based Port Error Handling**—If Cisco UCS Manager detects any errors on active IOM Network Interface (NIF) ports, and if the Error-disable setting is enabled, Cisco UCS Manager automatically disables the respective FI port that is connected to the IOM NIF port that had errors.

  When a FI port is error disabled, it is effectively shut down and no traffic is sent or received on that port.

- **Advanced Local Storage Configuration:**

  - Configuration of Storage Profiles and multiple virtual drives—To allow flexibility in defining the number of storage disks, roles and usage of these disks, and other storage parameters, you can create and use storage profiles. A storage profile encapsulates the storage requirements for one or more service profiles. You can also configure multiple virtual drives.

  - Configuration of a local LUN or a JBOD as the primary boot device

  - Support for local storage configuration on multiple storage controllers

  - Support for out-of-band configuration for local storage

- **Pass-through Capability for Gen 3 Fusion IO Mezzanine Cards**—Cisco UCS Manager now supports the pass-through capability of Gen 3 Fusion IO Mezzanine cards for blade servers. Pass-through for Mezzanine cards is a hardware capability that extends the available ports for the Cisco UCS VIC 1340 or VIC 1240 adapter though the Mezzanine slot, and brings the total I/O bandwidth of the VIC 1340 or VIC 1240 adapters to dual 4 x 10 GbE.

- **Fabric Interconnect Traffic Evacuation**—During upgrade, you can evacuate the secondary Fabric Interconnect traffic to ensure that there is no traffic flowing through the Fabric Interconnect from all servers attached to it through an IOM or FEX. This allows you to ensure that traffic will properly failover to the other Fabric Interconnect before you can proceed with the firmware upgrade.

- **Per Fabric Interconnect Chassis Reacknowledgment**—You can now reacknowledge a chassis per Fabric Interconnect. This allows you to maintain connectivity to the chassis through the other Fabric Interconnect.

- **TPM and TXT Configuration through UCSM**—The Trusted Platform Module (TPM) is a component that can securely store artifacts, such as passwords, certificates, or encryption keys, which are used to authenticate the server. A TPM can also be used to store platform measurements that help ensure that the platform remains trustworthy. Intel Trusted Execution Technology (TXT) provides greater protection for information that is used and stored on the server.

This release supports TPM and TXT configuration on Cisco UCS M4 blade and rack-mount servers through Cisco UCS Manager. TPM is enabled by default and TXT is disabled by default.

- **Consistent Device Naming Support**—Consistent Device Naming (CDN) allows Ethernet interfaces to be named in a consistent manner. This makes Ethernet interface names more persistent when adapter or other configuration changes are made.

Note CDN is supported only on Windows 2012 R2.

- **Fabric Scale Improvements**—Each Cisco UCS domain now supports:
    - Up to 8 appliance ports
    - 320 endpoints
    - Up to 320 vHBAs per Fabric Interconnect
- **Scriptable vMedia:**
    - You can configure the file name of the vMedia mount image to use the name of the service profile with which the vMedia policy is associated.
    - You can specify the authentication protocol to be used when you select CIFS as the communication protocol with the remote server.
- **Support for Service Profile Migration with UEFI Boot Mode**—When a service profile is migrated from one server to another, the BIOS on the destination server will continue to load the boot loader information and boot in UEFI boot mode.
- **NVGRE with IPv6 and VMQ**—You can enable NVGRE with VMQ and NVGRE with IPv6 on the same vNIC.
- **usNIC Support with Intel® MPI**—Intel® Message Passing Interface (MPI) is developed for high performance computing. You can now use the Intel MPI Library version 4 or 5 with Cisco user-space NIC (Cisco usNIC) for a low-latency and high-throughput communication transport.
- **Other Enhancements:**
    - While the infrastructure firmware is being upgraded, an automatic, internal, full state backup file is created.
    - When creating an SNMP trap, you can use an IPv4 address, or an IPv6 address, or a fully qualified domain name of an IPv4 address as the SNMP host name.
    - A new tech-support memory option is introduced to create a tech-support file with only server memory information gathered across the Cisco UCS domain.
    - When creating a server pool qualification policy, you can now specify the storage disk type as HDD, SSD or unspecified.

Release 2.2(3c) adds support for the following:

- QPI snoop mode via Service Profile

Release 2.2(3a) adds support for the following:

- Tiered Port-Licensing for direct-connect C-Series servers
- Smart Call Home Enhancements
- BIOS/CIMC secure boot support for C-series servers
- DIMM blacklisting support for C-series servers
- ENIC - DPDK Integration
- Stateless Offload for Overlay Networks (NVGRE / VXLAN)
- Monitoring of the IOM/FI interfaces
- LAN and SAN topology information
- usNIC support for IP-routable transport

Release 2.2(2c) adds support for the following:

- Scriptable vMedia
- NetFlow support
- PVLAN Enhancements
- Pre-Upgrade Validation Checks
- GPU Firmware Management
- Wear-Level Monitoring on Flash Adapters
- KVM/vMedia Client Enhancements
- Cisco VIC Driver Enhancements:
    - Adaptive Interrupt Coalescing (AIC)
    - Accelerated Receive Flow Steering (ARFS)
    - netQueue Support
- Support for ‘lacp suspend-individual’ on Uplink Port-Channel

Release 2.2(1b) adds support for the following:

- IPv6 Management support
- Cisco Integrated Management Controller (CIMC) In-band Management
- Fabric scaling: VLAN, VIFs, IGMP, Network Adapter Endpoints
- Uni-Directional Link Detection (UDLD) support

- User Space NIC (usNIC) for Low Latency
- Support for Virtual Machine Queue (VMQ)
- C-Series Servers Direct Connect to FI without FEX
- Two-factor Authentication for UCS Manager Logins
- VM-FEX for Hyper-V Management with Microsoft SCVMM
- Direct KVM Access
- Server Firmware Auto Sync
- Enhanced Local Storage Management
- Flash Adapters and HDD Firmware Management
- Precision Boot Order Control
- Secure Boot (B-series only)
- UEFI Boot Support
- FlexFlash (Local SD card) support
- Trusted Platform Module (TPM) Inventory
- DIMM Blacklisting and Correctable Error Reporting (B-series only)
- C-Series Board Controller Firmware Management

Note If you want to refer to a list of supported OS in this release, check the Hardware and Software Interoperability Matrix for this release.

Security Fixes

The following are security fixes in Cisco UCS Manager Release 2.2:

Table 6: Security Fixes in Release 2.2

Release	Defect ID	CVE (s)	Description
2.2(8m)	CSCvc22208	CVE-2018-0303	A vulnerability in the Cisco Discovery Protocol component of Cisco FXOS Software and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code as root, or cause a denial of service (DoS) condition on the affected device. The vulnerability exists because of insufficiently validated Cisco Discovery Protocol packet headers. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to a Layer 2 adjacent affected device. A successful exploit could allow the attacker to cause a buffer overflow, which could allow the attacker to execute arbitrary code as root, or cause a denial of service (DoS) condition on the affected device. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability. This advisory is available at the following link: Cisco FXOS and NX-OS Software Cisco Discovery Protocol Arbitrary Code Execution Vulnerability

Release	Defect ID	CVE (s)	Description
2.2(8m)	CSCve02433	CVE-2018-0314	A vulnerability in the Cisco Fabric Services (CFS) component of Cisco FXOS Software and Cisco NX-OS Software could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. The vulnerability exists because the affected software insufficiently validates Cisco Fabric Services packet headers when the software processes packet data. An attacker could exploit this vulnerability by sending a maliciously crafted Cisco Fabric Services packet to an affected device. A successful exploit could allow the attacker to cause a buffer overflow condition on the device, which could allow the attacker to execute arbitrary code on the device. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability. This advisory is available at the following link: Cisco FXOS and NX-OS Software Cisco Fabric Services Arbitrary Code Execution Vulnerability

Release	Defect ID	CVE (s)	Description
2.2(8m)	CSCve02461 CSCve41538	CVE-2018-0304 CVE-2018-0310	A vulnerability in the Cisco Fabric Services component of Cisco FXOS Software and Cisco NX-OS Software could allow an unauthenticated, remote attacker to obtain sensitive information from memory content, create a denial of service (DoS) condition, or execute arbitrary code as root. The vulnerability exists because the affected software insufficiently validates Cisco Fabric Services packet headers. An attacker could exploit this vulnerability by sending a crafted Cisco Fabric Services packet to an affected device. A successful exploit could allow the attacker to cause a buffer overflow or buffer overread condition in the Cisco Fabric Services component, which could allow the attacker to obtain sensitive memory content, create a DoS condition, or execute arbitrary code as root. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability. These advisories are available at the following links: Cisco FXOS and NX-OS Software Cisco Fabric Services Denial of Service Vulnerability Cisco FXOS and NX-OS Software Cisco Fabric Services Arbitrary Code Execution Vulnerability

Release	Defect ID	CVE (s)	Description
2.2(8m)	CSCve02787 CSCve02819	CVE-2018-0308 CVE-2018-0312	A vulnerability in the Cisco Fabric Services component of Cisco FXOS Software and Cisco NX-OS Software could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. The vulnerability exists because the affected software insufficiently validates header values in Cisco Fabric Services packets. An attacker could exploit this vulnerability by sending a crafted Cisco Fabric Services packet to an affected device. A successful exploit could allow the attacker to cause a buffer overflow, which could allow the attacker to execute arbitrary code or cause a DoS condition. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability. These advisories are available at the following links: Cisco FXOS and NX-OS Software Cisco Fabric Services Arbitrary Code Execution Vulnerability Cisco FXOS and NX-OS Software Cisco Fabric Services Arbitrary Code Execution Vulnerability

Release	Defect ID	CVE (s)	Description
2.2(8m)	CSCve41541 CSCve41593	CVE-2018-0311 CVE-2018-0305	A vulnerability in the Cisco Fabric Services (CFS) component of Cisco FXOS Software and Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability exists because the affected software insufficiently validates Cisco Fabric Services packets when the software processes packet data. An attacker could exploit this vulnerability by sending a maliciously crafted Cisco Fabric Services packet to an affected device. A successful exploit could allow the attacker to force a NULL pointer dereference or cause a buffer overflow condition on the device, which could cause process crashes and result in a DoS condition on the device. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability. These advisories are available at the following links: Cisco FXOS and NX-OS Software Cisco Fabric Services Denial of Service Vulnerability Cisco FXOS and NX-OS Software Cisco Fabric Services Denial of Service Vulnerability

Release	Defect ID	CVE (s)	Description
2.2(8m)	CSCvg71290	CVE-2018-0291	A vulnerability in the Simple Network Management Protocol (SNMP) input packet processor of Cisco NX-OS Software could allow an authenticated, remote attacker to cause the SNMP application on an affected device to restart unexpectedly. The vulnerability is due to improper validation of SNMP protocol data units (PDUs) in SNMP packets. An attacker could exploit this vulnerability by sending a crafted SNMP packet to an affected device. A successful exploit could allow the attacker to cause the SNMP application to restart multiple times, leading to a system-level restart and a denial of service (DoS) condition. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability. This advisory is available at the following link: Cisco NX-OS Software Authenticated Simple Network Management Protocol Denial of Service Vulnerability
2.2(8m)	CSCvj10183	CVE-2019-1616	A vulnerability in the Cisco Fabric Services component of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a buffer overflow, resulting in a denial of service (DoS) condition. The vulnerability is due to insufficient validation of Cisco Fabric Services packets. An attacker could exploit this vulnerability by sending a crafted Cisco Fabric Services packet to an affected device. A successful exploit could allow the attacker to cause a buffer overflow, resulting in process crashes and a DoS condition on the device. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability. This advisory is available at the following link: Cisco NX-OS Software Cisco Fabric Services Denial of Service Vulnerability

Release	Defect ID	CVE (s)	Description
2.2(8m)	CSCvm53116	CVE-2019-1599	A vulnerability in the network stack of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on the affected device. The vulnerability is due to an issue with allocating and freeing memory buffers in the network stack. An attacker could exploit this vulnerability by sending crafted TCP streams to an affected device in a sustained way. A successful exploit could cause the network stack of an affected device to run out of available buffers, impairing operations of control plane and management plane protocols, resulting in a DoS condition. This advisory is available at the following link: Cisco NX-OS Software Netstack Denial of Service Vulnerability
2.2(8m)	CSCvn61411	—	A vulnerability in the diagnostic CLI command of the Cisco UCS 6200 Series Fabric Interconnects may allow an authenticated local attacker to view sensitive information in the command output. The vulnerability is due to lack of proper masking of sensitive information before being written to the diagnostic support output. An attacker may exploit this vulnerability by authenticating to the targeted device and issuing a specific diagnostic CLI command. However, an attacker needs a valid user credentials to exploit this vulnerability. Cisco UCS Manager Release 2.2(8m) includes the fix for this issue. Password hashes that show in the CLI command are now hidden.

Release	Defect ID	CVE (s)	Description
2.2(8m)	CSCvp28016 CSCvp27917 CSCvo21412 CSCvp30013	CVE-2018-12126 CVE-2018-12127 CVE-2018-12130 CVE-2019-11091	

Release	Defect ID	CVE (s)	Description
			Cisco UCS M3 and M4 servers and Hyperflex M4 servers are vulnerable to variants of exploits that use Microarchitectural Data Sampling (MDS) to gain access to data being processed in the CPU by other applications. • CVE-2018-12126 (Microarchitectural Store Buffer Data Sampling) affects store buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Manager release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. • CVE-2018-12127 (Microarchitectural Load Port Data Sampling) affects load buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Manager release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. • CVE-2018-12130 (Microarchitectural Fill Buffer Data Sampling) affects line fill buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Manager release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. • CVE-2019-11091 (Microarchitectural Data Sampling Uncacheable Memory) affects uncacheable memory in the CPU, and 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 the follwing servers: • Cisco UCS M4 servers and Hyperflex M4 servers that are based on Intel® Xeon® Processor E5 v3 and v4 Product Family processors • Cisco UCS M4 servers and Hyperflex M4 servers that are based on Intel® Xeon® Processor E7 v2, v3, and v4 Product Family processors

Release	Defect ID	CVE (s)	Description
			• Cisco UCS B-Series M3 Blade Servers that are based on Intel® Xeon® Sandy Bridge E5-2600 and Ivy Bridge E5 2600 v2 Product Family processors These BIOS revisions include the updated microcode that is a required part of the mitigation for these vulnerabilities.
2.2(8m)	CSCvd34862	CVE-2018-0294	A vulnerability in the write-erase feature of Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to configure an unauthorized administrator account for an affected device. The vulnerability exists because the affected software does not properly delete sensitive files when certain CLI commands are used to clear the device configuration and reload a device. An attacker could exploit this vulnerability by logging into an affected device as an administrative user and configuring an unauthorized account for the device. The account would not require a password for authentication and would be accessible only via a Secure Shell (SSH) connection to the device. A successful exploit could allow the attacker to configure an unauthorized account that has administrative privileges, does not require a password for authentication, and does not appear in the running configuration or the audit logs for the affected device. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability. This advisory is available at the following link: Cisco FXOS and NX-OS Software Unauthorized Administrator Account Vulnerability

Release	Defect ID	CVE (s)	Description
2.2(8m)	CSCvk70633	CVE-2019-1962	A vulnerability in the Cisco Fabric Services (CFS) component of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause process crashes, which can result in a denial of service (DoS) condition on an affected system. The vulnerability is due to insufficient validation of TCP packets when processed by the Cisco Fabric Services over IP (CFSoIP) feature. An attacker could exploit this vulnerability by sending a crafted CFS TCP packet to an affected device. A successful exploit could allow the attacker to cause process crashes, resulting in a device reload and a DoS condition. Note: There are three distribution methods that can be configured for CFS. This vulnerability only affects distribution method CFSoIP, which is disabled by default. See the Security Advisory for more information. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability. This advisory is available at the following link: Cisco NX-OS Software Cisco Fabric Services over IP Denial of Service Vulnerability

Release	Defect ID	CVE (s)	Description
2.2(8m)	CSCvn52167	CVE-2019-1965	A vulnerability in the Virtual Shell (VSH) session management for Cisco NX-OS Software could allow an authenticated, remote attacker to cause a VSH process to fail to delete upon termination. This can lead to a build-up of VSH processes that overtime can deplete system memory. When there is no system memory available, this can cause unexpected system behaviors and crashes. The vulnerability is due to the VSH process not being properly deleted when a remote management connection to the device is disconnected. An attacker could exploit this vulnerability by repeatedly performing a remote management connection to the device and terminating the connection in an unexpected manner. A successful exploit could allow the attacker to cause the VSH processes to fail to delete, which can lead to a system-wide denial of service (DoS) condition. The attacker must have valid user credentials to log in into the device via the remote management connection. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability. This advisory is available at the following link: Cisco NX-OS Software Remote Management Memory Leak Denial of Service Vulnerability

Release	Defect ID	CVE (s)	Description
2.2(8l)	CSCvm02934	CVE-2018-3615 CVE-2018-3620 CVE-2018-3646	Cisco UCS B-Series M2 servers and 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 available here: CPU Side-Channel Information Disclosure Vulnerabilities: August 2018

Release	Defect ID	CVE (s)	Description
2.2(8l)	CSCvm03356	CVE-2018-3615 CVE-2018-3620 CVE-2018-3646	Cisco UCS B-Series M3 servers and C-Series M3 servers are based on Intel® processors that are vulnerable to exploits that use CPU speculative processing and data cache timing to potentially identify privileged information. These exploits are collectively known as L1 Terminal Fault (L1TF). • CVE-2018-3615 (affecting SGX), also known as Foreshadow, is not known to affect any existing Cisco UCS servers because Cisco UCS M5 and earlier generation servers, and HyperFlex M5 and earlier generation servers do not use Intel® SGX technology. • CVE-2018-3620 (affecting OS/System Management Mode) and CVE-2018-3646 (affecting Virtual Machine Monitors) are referred to as L1 Terminal Fault attacks by Intel®. These vulnerabilities are mitigated by applying the updated processor microcode from Intel® included in the server firmware bundle, and the relevant Operating System and Hypervisor patches from the appropriate vendors. This release includes BIOS revisions for Cisco UCS M3 generation servers. These BIOS revisions include the updated processor microcode that is a required part of the mitigation for CVE-2018-3620 (OS/SMM) and CVE-2018-3646 (VMM). Operating System and Hypervisor patches from the appropriate vendors may also be required to mitigate these vulnerabilities. For more information, please see the Cisco Security Advisory available here: CPU Side-Channel Information Disclosure Vulnerabilities: August 2018

Release	Defect ID	CVE (s)	Description
2.2(8l)	CSCvm03351	CVE-2018-3615 CVE-2018-3620 CVE-2018-3646	Cisco UCS B-Series M4 servers, C-Series M4 servers, S3260 M4 storage servers, and HyperFlex M4 servers are vulnerable to exploits that use CPU speculative processing and data cache timing to potentially identify privileged information. These exploits are collectively known as L1 Terminal Fault (L1TF). • CVE-2018-3615 (affecting SGX), also known as Foreshadow, is not known to affect any existing Cisco UCS servers because Cisco UCS M5 and earlier generation servers, and HyperFlex M5 and earlier generation servers do not use Intel® SGX technology. • CVE-2018-3620 (affecting OS/System Management Mode) and CVE-2018-3646 (affecting Virtual Machine Monitors) are referred to as L1 Terminal Fault attacks by Intel®. These vulnerabilities are mitigated by applying the updated processor microcode from Intel® included in the server firmware bundle, and the relevant Operating System and Hypervisor patches from the appropriate vendors. This release includes BIOS revisions for Cisco UCS M4 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 available here: CPU Side-Channel Information Disclosure Vulnerabilities: August 2018

Release	Defect ID	CVE (s)	Description
2.2(8l)	CSCvj54847 CSCvj54187	CVE-2018-3639 CVE-2018-3640	Cisco UCS M4 servers and Hyperflex M4 servers are based on Intel® processors that are vulnerable to variants of an exploit that uses CPU speculative processing and data cache timing to efficiently leak information, known as Spectre. CVE-2018-3639 (Spectre/Variant #4) and CVE-2018-3640 (Spectre/Variant #3a) are addressed by applying the updated processor microcode from Intel included in the server firmware bundle, and the relevant Operating System and Hypervisor patches from the appropriate vendors. This release includes BIOS revisions for Cisco UCS M4 and Hyperflex M4 generation servers. These BIOS revisions include the updated processor microcode that is a required part of the mitigation for CVE-2018-3639 (Spectre/Variant #4) and CVE-2018-3640 (Spectre/Variant #3a). For more information, see the Cisco Software Advisory at: CPU Side-Channel Information Disclosure Vulnerabilities: May 2018

Release	Defect ID	CVE (s)	Description
2.2(8l)	CSCvj54880	CVE-2018-3639 CVE-2018-3640	Cisco UCS M3 servers are based on Intel® processors that are vulnerable to variants of an exploit that uses CPU speculative processing and data cache timing to efficiently leak information, known as Spectre. CVE-2018-3639 (Spectre/Variant #4) and CVE-2018-3640 (Spectre/Variant #3a) are addressed by applying the updated processor microcode from Intel included in the server firmware bundle, and the relevant Operating System and Hypervisor patches from the appropriate vendors. This release includes BIOS revisions for Cisco UCS M3 generation servers. These BIOS revisions include the updated processor microcode that is a required part of the mitigation for CVE-2018-3639 (Spectre/Variant #4) and CVE-2018-3640 (Spectre/Variant #3a). For more information, see the Cisco Software Advisory at: CPU Side-Channel Information Disclosure Vulnerabilities: May 2018

Release	Defect ID	CVE (s)	Description
2.2(8l)	CSCvj59299 CSCvj59301	CVE-2018-3639 CVE-2018-3640	Cisco UCS M2 servers that are based on Intel® EP and EX Series processors 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 servers that are based on Intel® EP and EX Series processors. 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, see the Cisco Software Advisory at: CPU Side-Channel Information Disclosure Vulnerabilities: May 2018

Release	Defect ID	CVE (s)	Description
2.2(8l)	CSCvb86743	CVE-2018-0302	A vulnerability in the CLI parser of Cisco FXOS Software and Cisco Unified Computing (UCS) Fabric Interconnect Software could allow an authenticated, local attacker to cause a buffer overflow on an affected device. The vulnerability is due to incorrect input validation in the CLI parser subsystem. An attacker could exploit this vulnerability by exceeding the expected length of user input. A successful exploit could allow the attacker to execute arbitrary code with root privileges on the affected system. There are no workarounds that address this vulnerability. Cisco has released software updates that address this vulnerability. For more information, see the Cisco Security Advisory, which is available at the following link: Cisco FXOS Software and UCS Fabric Interconnect Arbitrary Code Execution Vulnerability

Release	Defect ID	CVE (s)	Description
2.2(8j)	CSCvh51224 CSCvg97965 CSCvg98015 CSCvg97979 CSCvh31576	CVE-2017-5715 CVE-2017-5753 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. • 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. • CVE-2017-5753 (Spectre/Variant 1) is addressed by applying relevant Operating System and Hypervisor patches from the appropriate vendors. This release includes BIOS revisions for Cisco UCS M2, M3, and M4 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, see the Cisco Security Advisory at https://tools.cisco.com/security/center/content/ CiscoSecurityAdvisory/cisco-sa- 20180104-cpusidechannel.
2.2(8i)	CSCvb61637 CSCvb86764 CSCvb86775 CSCvb86797 CSCvb86816	CVE-2017-6600 CVE-2017-6601 CVE-2017-6602 CVE-2017-6598 CVE-2017-6597	A vulnerability in the CLI of the Cisco Unified Computing System Manager could allow an authenticated, local attacker to perform a command injection attack. The security vulnerabilities are addressed.

Release	Defect ID	CVE (s)	Description
2.2(8i)	CSCvc37931	CVE-2017-6604	The following Cisco UCS Manager and Cisco Integrated Management Controller versions may be affected by the redirection vulnerabilities: For Unified Computing System (UCS) B-Series M3 and M4 Blade Servers, this affects any of the 2.2(8) and 3.1(2) blade bundle versions. None of the 3.0 or 3.1(1) blade bundle versions are affected. For Unified Computing System (UCS) C-Series M3 and M4 Rack Servers, this affects 3.0(1c) CIMC versions. None of the 1.5 or 2.0 CIMC versions are affected.
2.2(8i)	CSCuz52483	CVE-2016-2105 CVE-2016-2106 CVE-2016-2107 CVE-2016-2108 CVE-2016-2109	Cisco UCS Manager may be affected by the following vulnerabilities: • CVE-2016-2105 EVP_EncodeUpdate overflow • CVE-2016-2106 EVP_EncryptUpdate overflow • CVE-2016-2107 Padding oracle in AES-NI CBC MAC check • CVE-2016-2108 Memory corruption in the ASN.1 encoder • CVE-2016-2109 ASN.1 BIO excessive memory allocation Cisco UCS Manager is not affected by the following vulnerability: • CVE-2016-2176 EBCDIC overread
2.2(8i)	CSCuu83383	CVE-2015-1788 CVE-2015-1789 CVE-2015-1790 CVE-2015-1791 CVE-2015-1792 CVE-2014-8176	The OpenSSL vulnerabilities with Cisco UCS Manager identified by the Common Vulnerability and Exposures (CVE) IDs listed are fixed.

Release	Defect ID	CVE (s)	Description
2.2(8i)	CSCvc94686 CSCvc96103	CVE-2017-3731	The OpenSSL vulnerabilities with Cisco UCS Manager identified by the Common Vulnerability and Exposures (CVE) IDs listed are fixed. Cisco UCS Manager 2.2 may be affected by the following vulnerability: • CVE-2017-3731 Truncated packet could crash via OOB read Cisco UCS Manager is not affected by the following vulnerabilities: • CVE-2017-3730 DHE parameters cause a client crash • CVE-2017-3732 BN_mod_exp may produce incorrect results on x86_64 • CVE-2017-3733 A truncated packet may cause the server or client to perform an out-of-bounds read
2.2(8i)	CSCvb48577 CSCvb48644	CVE-2016-2177 CVE-2016-2178 CVE-2016-2179 CVE-2016-2180 CVE-2016-2181 CVE-2016-2182 CVE-2016-2183 CVE-2015-4000 CVE-2016-6303 CVE-2016-6302 CVE-2016-6304 CVE-2016-6305 CVE-2016-6306 CVE-2016-6307 CVE-2016-6308 CVE-2016-6309 CVE-2016-7052	The latest CiscoSSL 6.1.188-fips (corresponding to OpenSSL 1.0.2k, and detailed in CSCvc94686) now automatically fixes the OpenSSL vulnerabilities identified by one or more of the Common Vulnerability and Exposures (CVE) IDs listed.

Release	Defect ID	CVE (s)	Description
2.2(8i)	CSCux41398	CVE-2015-3194 CVE-2015-3195	The OpenSSL vulnerabilities with Cisco UCS Manager identified by the Common Vulnerability and Exposures (CVE) IDs listed are fixed. Cisco Unified Computing System B-Series (Blade) Servers are affected by: • CVE-2015-3194 • CVE-2015-3195 Cisco Unified Computing System B-Series (Blade) Servers are not affected by: • CVE-2015-1794 • CVE-2015-3193 • CVE-2015-3196
2.2(8i)	CSCvc88543	• CVE-2016-0736 • CVE-2016-2161 • CVE-2016-5387 • CVE-2016-8740 • CVE-2016-8743	The following CVEs do not apply to Cisco UCS Manager 2.2(8) because the relevant modules are not compiled as part of the Apache HTTP server used in Cisco UCS Manager: • CVE-2016-0736 • CVE-2016-2161 • CVE-2016-5387 • CVE-2016-8740 CVE-2016-8743 is only applicable when backend servers are used. This does not affect Cisco UCS Manager Release 2.2(8).
2.2(8i)	CSCvf27392	• CVE-2017-3167 • CVE-2017-3169 • CVE-2017-7659 • CVE-2017-7668 • CVE-2017-7679	The Apache vulnerabilities with Cisco UCS Manager identified by the Common Vulnerability and Exposures (CVE) IDs listed are fixed.

Release	Defect ID	CVE (s)	Description
2.2(8i)	CSCvd72179	• CVE-2017-6464 • CVE-2017-6462 • CVE-2017-6463 • CVE-2017-6458 • CVE-2017-6451 • CVE-2017-6460 • CVE-2016-9042 • CVE-2017-6455 • CVE-2017-6452 • CVE-2017-6459 • CVE-2015-8138 • CVE-2016-7431	Cisco UCS Manager included a version of NTPd that was affected by the vulnerability identified by one or more of the following Common Vulnerability and Exposures (CVE) IDs. These CVE IDs no longer impact any Cisco UCS Manager release: • CVE-2017-6464—NTP-01-016 NTP: Denial of Service via Malformed Config • CVE-2017-6462—NTP-01-014 NTP: Buffer Overflow in DPTS Clock • CVE-2017-6463—NTP-01-012 NTP: Authenticated DoS via Malicious Config Option • CVE-2017-6458—NTP-01-004 NTP: Potential Overflows in ctl_put() functions • CVE-2017-6451—NTP-01-003 Improper use of snprintf() in mx4200_send() • CVE-2017-6460—NTP-01-002 Buffer Overflow in ntpq when fetching reslist • CVE-2016-9042—Network Time Protocol Origin Timestamp Check Denial of Service Vulnerability Cisco UCS Manager is not affected by the following CVE IDs: • CVE-2017-6455—NTP-01-009 NTP: Windows: Privileged execution of User Library code • CVE-2017-6452—NTP-01-008 NTP: Windows Installer: Stack Buffer Overflow from Command Line • CVE-2017-6459—NTP-01-007 NTP: Windows Installer: Data Structure terminated insufficiently • CVE-2015-8138—Zero Origin Timestamp Bypass • CVE-2016-7431—Zero Origin Timestamp Bypass

Release	Defect ID	CVE (s)	Description
2.2(8a)A	CSCvf35705	CVE-2017-9788 CVE-2017-9789	The vulnerabilities identified by the Common Vulnerability and Exposures (CVE) IDs listed are applicable only when mod_http2 and mod_auth_digest modules are used in the Apache server. The Apache server used by Cisco UCS Manager does not use mod_http2 and mod_auth_digest modules. Hence, the vulnerabilities identified by both CVE IDs listed do not impact any Cisco UCS Manager release.
2.2(3l)A	CSCvb85544	CVE-2016-5195	The security vulnerability is addressed.
2.2(8c)A	CSCuz91263	CVE-2016-6402	The security vulnerability is addressed.
2.2(8a)A	CSCuz92668	CVE-2016-4957 CVE-2016-4953 CVE-2016-4954 CVE-2016-4955 CVE-2016-4956	The security vulnerabilities are addressed.
2.2(3e)A	CSCus69458	CVE-2015-0235	The heap-based buffer overflow vulnerability in the GNU C library is addressed.
2.2(3d)A	CSCur29264	CVE-2014-3566	The security vulnerability is addressed.
2.2(3b)A	CSCur01379	CVE-2014-7169 CVE-2014-6271 CVE-2014-6277 CVE-2014-7186 CVE-2014-7187 CVE-2014-6278	The security vulnerabilities are addressed.
2.2(6c)B	CSCuq77241	CVE-2015-4265	The security vulnerability is addressed.
2.2(7b)	CSCut46044	CVE-2015-0286 CVE-2015-0287 CVE-2015-0289 CVE-2015-0292 CVE-2015-0293 CVE-2015-0209 CVE-2015-0288	The security vulnerabilities are addressed.

Release	Defect ID	CVE (s)	Description
2.2(7c)	CSCux95107	CVE-2015-7973 CVE-2015-7974 CVE-2015-7975 CVE-2015-7976 CVE-2015-7977 CVE-2015-7978 CVE-2015-7979 CVE-2015-8138 CVE-2015-8139 CVE-2015-8140 CVE-2015-8158	The security vulnerabilities are addressed.

Resolved Caveats

The resolved bugs for a release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains up-to-date information about bugs and vulnerabilities in this product and other Cisco hardware and software products.

Note You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. If you do not have one, you can register for an account.

For more information about the Cisco Bug Search Tool, see the Bug Search Tool Help & FAQ.

Resolved Caveats in Release 2.2(8m)

The following caveats are resolved in Release 2.2(8m):

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvk71319	The VIM process core causes Fabric Interconnect reboot. This issue has been resolved.	2.2(8l)A 3.2(3g)A	2.2(8m)A 3.2(3h)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvk63036	Unable to form a SAN port-channel between a Cisco UCS Fabric Interconnect pair and a Cisco Fibre Channel switch, where the Organizationally Unique ID (OUI) of the switch is one of the following: • 003a9c • 000831 • d0a5a6 This issue has been resolved.	2.2(3k)A 3.2(3d)A 4.0(2a)A	2.2(8m)A 3.2(3i)A 4.0(2b)A
CSCvf03280	When Cisco Fabric Services (CFS) distribution is enabled on UCS 6200 Series Fabric Interconnects, the Fabric Interconnect may reload due to a CFS process crash. This issue has been resolved.	2.2(8g)A	2.2(8m)A
CSCvg75477	After upgrading to Java 10, the Java GUI for Cisco UCS Manager could not be launched. This issue has been resolved, and the Java GUI for Cisco UCS Manager can now be launched using Java 10. **Note** To use Java 9 and later versions, end user licenses are required from Oracle.	2.2(8i)A	2.2(8m)A

Resolved Caveats in Release 2.2(8l)

The following caveats are resolved in Release 2.2(8l):

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvi98058	New OS installation in UEFI mode and BIOS version 2.2.6f.0 no longer fails.	3.1(3h)B	2.2(8l)B 3.1(3j)B
CSCvg64592	Rack servers integrated with 6200 Series FI have connectivity after reboot of the subordinate FI, if the VLAN range (expressed as a string of characters) applied on a port-profile exceeds 255 characters.	3.1(3c)A	2.2(8l)A 3.1(3j)A 3.2(3a)A

Resolved Caveats in Release 2.2(8j)

The following caveats are resolved in Release 2.2(8j)

Table 7: Resolved Caveats in Release 2.2(8j)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvh22485	In a VMFEX setup with PVLAN host configurations on the Veths, after vMotion or VM migration, VMs were unable to receive broadcast or multicast packets, including ARP packets. This issue has been resolved.	2.2(8g)A	2.2(8j)

Resolved Caveats in Release 2.2(8i)

The following caveats are resolved in Release 2.2(8i).

Table 8: Resolved Caveats in Release 2.2(8i)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvg44307	Communication between two end hosts no longer fails within the same VLAN and fabric interconnect.	2.2(4b)A	2.2(8i)A
CSCux49157	UCS Manager now has a user configurable option to select the TLS version.	2.2(6d)A	2.2(8i)A
CSCuz98957	UCS Manager no longer incorrectly reports the amount of drive slots on B200-M2 blade servers.	2.2(7b)A	2.2(8i)A
CSCva31113	After a fabric interconnect reboot, the fabric interconnect may not fully boot and become network accessible. The Serial Console connection to the fabric interconnect may show a 'loader' prompt or show initial configuration prompts.	2.2(3d)A	2.2(8i)A
CSCvb00303	During a Server discovery, Rack servers no longer get stuck and may not discover due to a lost connection status from the B side while only A side is appearing. This may occur after upgrading to 2.2(8b) and performing an Erase Samdb operation and then enabling all required server ports to bring the server up.	2.2(8b)A	2.2(8i)A
CSCvc58789	A port no longer shows a disabled error after 10 consecutive DFE tuning failures.	2.2(8c)A	2.2(8i)A
CSCvc92275	A kernel panic no longer occurs on the fabric interconnect which could cause a reboot. The following command: `show logging onboard stack-trace` Shows that the panic may occur in the process usd_mts_kthread. The call trace can be reviewed for a full match to this defect.	2.2(6e)A	2.2(8i)A
CSCvd02546	During a UCS Manager upgrade from 2.2(3l) to 3.1(2) only the secondary fabric interconnect may be upgraded.	2.2(1b)A	2.2(8i)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvd54116	Setting a custom cipher suite for UCS Manager HTTPS to remove the usage of TLS v1.0 and 1.1, no longer results in a "handshake failure" error message when attempting to open a Java login to UCS Manager or a KVM session to a blade server.	2.2(8c)A	2.2(8i)A
CSCve19522	UCS domains running version 3.1(3a) no longer moves to a state of lost visibility after a certificate is regenerated on UCS Central and is able to recover. In some cases, the UCS 3.1(3a) domain registration may also get stuck in a registering state.	2.2(8g)A	2.2(8i)A
CSCvg06830	After adding a secondary fabric interconnect to a standalone setup and converting it to clustered setup, the VLAN 1 may not be added to the uplink port-channel, and no longer causes the vEth on the B side to fail pinning and render the subordinate fabric interconnect unusable.	2.2(6c)A	2.2(8i)A
CSCvc88543	Cisco UCS Manager includes a version of the Apache HTTP Server software that no longer affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs: • CVE-2016-0736 • CVE-2016-2161 • CVE-2016-5387 • CVE-2016-8740 • CVE-2016-8743	2.2(6c)A	2.2(8i)A
CSCuu83383 CSCvb48644	UCS Manager includes a version of OpenSSL that is no longer affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) IDs: • CVE-2015-4000 • CVE-2015-1788 • CVE-2015-1789 • CVE-2015-1790 • CVE-2015-1791 • CVE-2015-1792 • CVE-2014-8176	1.1(1j)A	2.2(8i)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCux41398	UCS Manager includes a version of OpenSSL that is no longer affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) IDs: • CVE-2015-3193 • CVE-2015-3194 • CVE-2015-3195 • CVE-2015-3196 • CVE-2015-1794	2.2(3a)B	2.2(8i)B
CSCuz52483	UCS Manager includes a version of OpenSSL that is no longer affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) IDs: • CVE-2016-2108 • CVE-2016-2107 • CVE-2016-2105 • CVE-2016-2106 • CVE-2016-2109 • CVE-2016-2176	2.2(8a)A	2.2(8i)A
CSCvb48577	UCS Manager includes a version of OpenSSL that is no longer affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) IDs: 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 And disclosed in https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160927-openssl	2.2(8g)B	2.2(8i)B

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvc94686	UCS Manager includes a version of OpenSSL that is no longer affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) IDs: • CVE-2017-3731 - Truncated packet could crash via OOB read This product is not affected by the following vulnerabilities: • CVE-2017-3730 - DHE parameters cause a client crash • CVE-2017-3732 - BN_mod_exp may produce incorrect results on x86_64	2.2(8g)A	2.2(8i)A
CSCvc96103	UCS Manager includes a version of OpenSSL that is no longer affected by the vulnerability identified by one or more of the following Common Vulnerability and Exposures (CVE) IDs: • CVE-2017-3731 • CVE-2017-3730 • CVE-2017-3732 And disclosed in https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170130-openssl	2.2(8g)A	2.2(8i)A
CSCvb61637	A vulnerability in the CLI of the Cisco Unified Computing System Manager could allow an authenticated, local attacker to perform a command injection attack. The vulnerability is due to insufficient input validation for the affected command. An authenticated local attacker could exploit this vulnerability by injecting crafted command arguments into a redirect of a vulnerable CLI command. An exploit could allow the attacker to execute arbitrary system commands with the privileges of the authenticated user. UCS Manager is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) IDs: CVE-2017-6600	2.2(8g)A	2.2(8i)A
CSCvb86764	A vulnerability in the CLI of the Cisco UCS Manager could allow an authenticated, local attacker to perform a command injection attack. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by injecting crafted command arguments into a vulnerable CLI command. An exploit could allow the attacker to read or write arbitrary files at the user's privilege level outside of the user's path. UCS Manager is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) IDs: CVE-2017-6601	2.2(8g)A	2.2(8i)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvb86775	A vulnerability in CLI of the Cisco Unified Computing System Manager could allow an authenticated, local attacker to perform a command injection attack. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by injecting crafted command arguments into a vulnerable CLI command. An exploit could allow the attacker to read or write arbitrary files at the user's privilege level outside the expected path and gain access to other devices. The vulnerability is identified by the following Common Vulnerability and Exposures (CVE) IDs: CVE ID CVE-2017-6602	2.2(8g)A	2.2(8i)A
CSCvb86797	A vulnerability in the debug plugin functionality of the Cisco Unified Computing System Manager could allow an authenticated, local attacker to execute arbitrary commands. The vulnerability is due to inadequate integrity checks for the debug plugin. An attacker could exploit this vulnerability by crafting a debug plugin and load it using elevated privileges. An exploit could allow the attacker to run malicious code that would allow for the execution of arbitrary commands as root. The vulnerability is identified by the following Common Vulnerability and Exposures (CVE) IDs: CVE ID CVE-2017-6598	2.2(8g)A	2.2(8i)A
CSCvb86816	A vulnerability in local-mgmt CLI of the Cisco Unified Computing System Manager could allow an authenticated, local attacker to perform a command injection attack. The vulnerability is due to insufficient input validation for the affected command. An authenticated local attacker could exploit this vulnerability by injecting crafted command arguments into a vulnerable CLI command. An exploit could allow the attacker to execute arbitrary system commands with the privileges of the authenticated user. The vulnerability is identified by the following Common Vulnerability and Exposures (CVE) IDs: CVE ID CVE-2017-6597	2.2(8g)A	2.2(8i)A
CSCvc37931	Unvalidated redirects and forwards may be possible when UCS Manager accepts untrusted input that could cause it to redirect the request to a URL contained within untrusted input. By modifying untrusted URL input to a malicious site, an attacker may successfully launch a phishing scam and steal user credentials. Unvalidated redirect and forward attacks can also be used to maliciously craft a URL that would pass the applications access control check and then forward the attacker to privileged functions that they would normally not be able to access. The vulnerability is identified by the following Common Vulnerability and Exposures (CVE) IDs: CVE ID CVE-2017-6604	2.2(8g)A	2.2(8i)A

Resolved Caveats in Release 2.2(8g)

The following caveats are resolved in Release 2.2(8g)

Table 9: Resolved Caveats in Release 2.2(8g)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCva14937	M4 blades installed with SD cards instead of a hard disk no longer halt at 'Local Drive' for automated deployments with the following boot policy: Boot Policy • CD/DVD • Local Drive • Network Adapter (PXE)	2.2(3f)B	2.2(8g)B
CSCvb85331	The following fault no longer occurs after a UCS Manager software upgrade. Code: F1781 Description: Management database version mismatch detected failover may not complete Affected Object: sys/mgmt-entity-B Name: Mgmt Entity Mgmt Db Version Mismatch Cause: Replication Failure Type: Management	2.2(8c)A	2.2(8g)A
CSCvc39322	For B260 M4 Blades, BIOS v3.1.2.2 no longer intermittently fails Windows HLK and HCK Trusted Platform Module (TPM) tests on Windows Server 2016 and Windows Server 2012 R2.	2.2(7b)B	2.2(8g)B
CSCvc10791	A DME process no longer crashes when the dynamic vNIC and static vNIC contain a different adminVcon property value.	2.2(3e)A	2.2(8g)A
CSCvc89242	The Fabric Interconnect no longer reboots due to a CDP process crash.	2.2(6e)A	2.2(8g)A
CSCvc46313	The remote operation of making the LUN online from UCS Central no longer fails with the error message: `Global Service profile [org-root/org-GKDC/org-<name>/ls-SP_3260_03] can not be modified from UCS domain. Please make the changes from UCS Central that you are registered with.`	2.2(4b)A	2.2(8g)A
CSCvc60876	The 6248, 6296, and 6332 Series Fabric Interconnects no longer sends Smart Call Home messages in the wrong format.	2.2(8b)A	2.2(8g)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvc31867	When upgrading the SSD to firmware 32F3Q, the firmware is no longer truncated and written as 2F3Q, which may cause a second request for the reboot of the server.	2.2(8a)A	2.2(8g)A
CSCux96072	During heavy I/O traffic, the Cisco 12G Modular RAID controller no longer goes offline with the Storage Controller SLOT HBA inoperable error logged in CIMC event logs.	2.2(6e)C	2.2(8g)C
CSCvc48423	Downloading a bundle more than 1GB in size from a local desktop no longer fails.	2.1(1a)A	2.2(8g)A

Resolved Caveats in Release 2.2(8f)

The following caveats are resolved in Release 2.2 (8f)

Table 10: Resolved Caveats in Release 2.2(8f)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuy81688	From Cisco UCS Manager tech-support, running **/var/sysmgr/sam_logs/httpd_cimc.log** on the affected fabric interconnect no longer shows the exceeded max time without restart error. From Cisco UCS Manager tech-support, running **/ls_l.out** on the affected fabric interconnect no longer shows the existence of a 'cimcrestart' file under /isan/apache/conf/. The modified date is now updated.	2.2(8a)A	2.2(8f)A
CSCuz53730	UCSM httpd process no longer experiences high memory usage or crash with a core file showing indications of memory allocation failure.	2.2(2c)A	2.2(8f)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCva35757	Latency between the UCS Manager Client and fabric interconnect no longer causes the firmware page to load slowly.	2.2(7b)A	2.2(8f)A
CSCvb11667	Server with UEFI BIOS enabled, no longer fails to SAN boot from a target LUN with an ID other than 0 and using T10 DIF protection.	2.2(8d)B	2.2(8f)B
CSCvb16804	Booting from SAN to 4K UEFI target no longer fails.	2.2(8a)B	2.2(8f)B
CSCvb08928	A fabric interconnect no longer reboots on VLAN deletion due to a FWM hap reset.	2.2(5a)A	2.2(8f)A
CSCvb78971	When attempting the auto-install of UCS Manager, the fabric interconnect upgrade no longer fails when the /var/tmp usage exceeds 10%.	2.2(3k)A	2.2(8f)A
CSCvb82862	EUI-64 bit addresses are now valid for storage connection policies or SAN boot targets.	2.2(8d)A	2.2(8f)A
CSCvb95978	On C460 M4 servers, TPM version 1.2 no longer fails to initialize after installing ESXi OS, and enabling and activating TPM and TXT.	2.2(8d)B	2.2(8f)B
CSCvc17769	The fabric interconnect no longer crashes when the bound interface of a Veth is in the Not Initialized State during a VLAN configuration change.	2.2(7c)A	2.2(8f)A

Resolved Caveats in Release 2.2 (8d)

The following caveats are resolved in Release 2.2 (8d)

Table 11: Resolved Caveats in Release 2.2 (8d)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvb05762	UCS Manager GUI and CLI no longer fail to respond when the Data Management Engine (DME) hangs with a `WaitOnLimit` log message.	2.2(7b)A	2.2(8d)A

Resolved Caveats in Release 2.2 (8d)T

The following caveats are resolved in Release 2.2 (8d)T

Table 12: Resolved Caveats in Release 2.2 (8d)T

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCva53726	UCS Manager no longer allows the downgrade of firmware for the following rack servers installed with v4 CPU models to a version less than the minimum required version of CIMC / BIOS firmware: • UCSC-C240-M4L • UCSC-C240-M4S • UCSC-C240-M4S • UCSC-C240-M4SX • UCSC-C220-M4L • UCSC-C220-M4S • UCSC-C240-M4SNEBS After a downgrade, servers no longer fail the BIOS post.	2.2(7c)T	2.2(8d)T

Resolved Caveats in Release 2.2 (8c)

The following caveats are resolved in Release 2.2 (8c)

Table 13: Resolved Caveats in Release 2.2 (8c)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuu29425	In RHEL 7.0 and 7.1 the ENIC driver now properly handles packets received on the native VLAN.	2.2(4b)B	2.2(8c)B
CSCuw50361	While collecting IOM tech-support by using the show platform software satctrl global output from the IOM, the HIF/NIF interfaces of an IOM no longer flap due to SDP heartbeat timeout.	2.2(4b)A	2.2(8c)A
CSCux11611	Seagate hard drives left spinning idle without an operating system installed or setup with the JBOD configuration without read or write activity are no longer prone to failure. Impacted hard drives are listed here: • UCS-HD4T7KS3-E • UCSC-C3X60-HD4TB (4TB) • UCS-HDD3TI2F214 (3TB) • UCS-HDD2TI2F213 (2TB) • UCS-HDD1TI2F212 (1TB) • UCS-HD6T7KL4K • UCSC-C3X60-HD6TB • UCSC-C3X60-6TBRR	2.2(7c)B	2.2(8c)B

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuy79306	When Cisco UCS C-Series servers with VIC 1225 or VIC 1227 are directly connected to Cisco Nexus 9000 switches, after making a large change on a switch, ports no longer flap or show as down on the switch but up on the server.	2.2(3f)B	2.2(8c)B
CSCuz41121	When booting to RHEL or running system stress tests, Cisco UCS B420 M4 servers with certain Intel ® E5 v3 CPUs no longer report QPI Correctable System Event Logs with the following error message: Link Layer CRC successful reset with no degradation	2.2(8a)B	2.2(8c)B
CSCuz91263	A vulnerability in the command-line interface (CLI) of the Cisco UCS Manager and UCS 6200 Series Fabric Interconnects is resolved.	2.2(1a)A	2.2(8c)A
CSCuz96855	UCS M71KR cards no longer crashes with the error “E4194871”.	2.2(6e)B	2.2(8c)B
CSCva27558	In scenarios such as traffic loops in external networks, a series of MAC add or delete operations no longer causes the MAC address to display in the software table, and nor in the hardware table for all the ASICs.	2.2(5c)A	2.2(8c)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCva34343	UCS Manager no longer reports false alerts due to P0V75_STBY sensor in Cisco B200 and M4 Blade Servers.	2.2(6e)B	2.2(8c)B
CSCva38476	An infrastructure software upgrade to UCS Manager 2.2(7b) or higher no longer fails when both fabric interconnects are incompatible or when one of the fabric interconnects is unresponsive.	2.2(7b)A	2.2(8c)A
CSCva71801	UCS Manager no longer fails to synchronize with IPv6 NTP server.	2.2(8a)A	2.2(8c)A
CSCva96740	Changes in adapter policy from UCS Manager now triggers a server redeploy.	2.2(8b)A	2.2(8c)A
CSCvb35827	Upgrade failure no longer occurs when a Cisco UCS system is configured with more than 128 LDAP groups and upgrade is performed either from Cisco UCS Manager Release 2.2.8 to Cisco UCS Manager Release 3.1(2b) or from Cisco UCS Manager Release 3.1(2b) to a later release.	2.2(8a)A	2.2(8c)A

Resolved Caveats in Release 2.2 (8b)

The following caveats are resolved in Release 2.2 (8b)

Table 14: Resolved Caveats in Release 2.2 (8b)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuu40978	The syslog is now truncated after it reaches the configured maximum size. It no longer fills up the Fabric Interconnect file system.	2.2(3d)A	2.2(8b)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuz54661	Cisco B200 M3 Server no longer fails to post if NUMA is disabled.	2.2(6g)B	2.2(8b)B
CSCuz86450	The server no longer reboots because the system does not accept user input on the order property of adaptorHostIf.	1.4(1j)A	2.2(8b)A
CSCva08256	Cisco CIMC and BIOS no longer get stuck updating or activating with the host firmware pack when the new host firmware pack has the same name and version as the system being updated.	2.2(7b)A	2.2(8b)A
CSCva34426	Cisco UCS 3X60 Server no longer fails to boot from LSI RAID controller managed disk slots 1 or 2, when the disks are in JBOD mode.	2.2(7c)A	2.2(8b)A
CSCva36835	A board controller update now ensures proper functionality of the LSI controller during a warm reboot or reset signal when using the Cisco B460 M4 or B260 M4 blade servers.	2.2(8a)B	2.2(8b)B
CSCva54957	A reboot is no longer triggered without a “user -ack” when modifying a service profile that requires a reboot while shallow association is failing.	2.1(3a)A	2.2(8b)A
CSCva67159	Cisco UCS Manager httpd no longer fails to start when the default keyring was deleted.	2.2(8a)A	2.2(8b)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCva72096	Cisco UCS servers running Intel E5 Xeon v4 CPUs no longer crash with a signature pointing to internal parity errors, page fault, general detect, or undefined opcode exceptions.	2.2(4b)B	2.2(8b)B
CSCva87230	A temporary loss in server connectivity no longer occurs when performing a Cisco UCS Manager upgrade to release 2.2(8a) from a build that does not contain the fix for CSCuq57142.	2.2(8a)A	2.2(8b)A

Resolved Caveats in Release 2.2 (8a)

The following caveats are resolved in Release 2.2 (8a)

Table 15: Resolved Caveats in Release 2.2 (8a)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuv13019	When the desired power state of a service profile was set to Power ON, and Cisco UCS Manager triggered shallow discovery for the blade server, server shutdown from the OS was powered ON by Cisco UCS Manager. This issue is now resolved.	2.1(1f)B	2.2(8a)B
CSCuv31912	UCS Manager iptables are no longer duplicating rules in the FORWARD table.	2.2(3d)A	2.2(8a)A
CSCuw16950	FSM failures no longer trigger the addition of duplicate entries in IP tables.	2.2(3b)A	2.2(8a)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCux59912	A Cisco UCS system with servers connected to a Cisco Nexus 2232 FEX no longer experiences bladeAG cores.	2.2(5c)C	2.2(8a)C
CSCux63909	FC abort is no longer observed while running uplink port flap test on uplink Ethernet port-channel from an FI to a Cisco Nexus 7000 switch.	2.0(2m)B	2.2(8a)B
CSCuy98678	Cisco UCS 6296 fabric interconnect no longer crashes unexpectedly with kernel panic, and impact any devices connected the fabric interconnect.	2.2(6c)A	2.2(8a)A
CSCuz92668	Vulnerabilities affecting various versions of NTPd are now resolved.	2.2(1a)A	2.2(8a)A
CSCva04106	Removing a SAN port channel member no longer causes SAN ports to go down.	2.2(3d)A	2.2(8a)A

Resolved Caveats in Release 2.2 (7e)

The following caveats are resolved in Release 2.2 (7e)

Table 16: Resolved Caveats in Release 2.2 (7e)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCva72096	Cisco UCS servers running Intel E5 Xeon v4 CPUs no longer crash with a signature pointing to internal parity errors, page fault, general detect, or undefined opcode exceptions.	2.2(4b)B	2.2(7e)B

Resolved Caveats in Release 2.2(7d)

The following caveats are resolved in Release 2.2(7d)

Table 17: Resolved Caveats in Release 2.2(7d)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuz69100	Disk Firmware update no longer fails for local disks on a C240 rack server that has an UCSC-SAS12GHBA storage controller.	2.2(7b)A	2.2(7d)A
CSCuz86450	The server no longer reboots because the system does not accept user input on the order property of adaptorHostIf.	1.4(1j)A	2.2(7d)A
CSCuz65286	Cisco UCS Manager firmware upgrade failed with the following message UCSM upgrade validation failed when the default value for IO throttle count in the FC adapter policy had a value of 16. This issue is resolved. The default IO throttle count is now set to 256.	2.2(3a)A	2.2(7d)A
CSCuv45574	After downgrading the controller firmware on C220/C240 M3 systems with LSI 9271-8i controller, the GUID of virtual disks no longer change and the virtual machines running on the ESXi OS no longer become inaccessible.	2.2(6f)A	2.2(7d)A
CSCux53224	A fatal error may be observed when creating or removing virtual drives with RAID 5 and RAID 6 controller combinations. This issue is now resolved.	2.2(7c)C	2.2(7d)C

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCva01733	PXE in Legacy Boot mode no longer hangs with excessive unicast or multicast high background traffic with a packet size larger than MTU directed to the client server. This was seen with ESXi Autodeploy on a specific setup which likely had unusually high multicast traffic directed at the client server. This traffic was not from the PXE server for file transfer, but from some other source.	2.2(6e)B	2.2(7d)B
CSCva29365	Enabling stateless offloads for NVGRE in the following 3rd generation Cisco VIC adapters' configuration with UCSM/CIMC no longer leads to inaccessible vNIC interfaces in the host OS: • UCSC-C3260-SIOC • UCSB-VIC-M83-8P • UCSB-MLOM-40G-02 • UCSB-MLOM-40G-03 • UCSC-PCIE-C40Q-03 • UCSC-MLOM-C40Q-03	2.2(7b)B	2.2(7d)B

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuu40291	When debug logging is enabled, Cisco UCS Manager tech-support showed that syslogd_debug files were present, but the show debug logfile syslogd_debugs CLI command failed with the following error: `Logfile(syslogd_debugs) does not exist` This issue is now resolved.	2.2(3a)A	2.2(7d)A
CSCuu40978	The Fabric Interconnect file system previously generated too many syslog messages and prevented further logging. This issue is now resolved.	2.2(3d)A	2.2(7d)A
CSCuz20650	When syslog messages are generated continuously, the syslog suspend timer does not recover. Thus, no events are sent to the remote syslog server. This issue is now resolved.	2.2(3a)A	2.2(7d)A

Resolved Caveats in Release 2.2 (7c)

The following caveats are resolved in Release 2.2 (7c)

Table 18: Resolved Caveats in Release 2.2 (7c)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCul97240	When a UCS rack server is present in a UCS setup, DHCP renewal now triggers Information level syslog messages to be sent to the syslog server configured on Cisco UCS Manager.	2.2(1a)A	2.2(7c)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuq57142	In a port channel universe, the following no longer happen: • A port channel ID may sometimes not be released after use. This could eventually lead to the universe of port channel IDs being empty, and no port channel IDs being available for use. • After an upgrade, power loss, FI reboot or failover, the empty port channel universe is incorrectly interpreted as a new installation, and repopulated. This leads to duplicate port channel ID allocation when a server is attached to the FI, or when a server is re-acknowledged.	2.2(3a)A	2.2(7c)A
CSCuq74472	Unnecessary thermal events on IOM stating “Thermal sensor reading not available” are no longer seen.	2.1(3c)B	2.2(7c)B
CSCux58865	DIMM temperature readings are no longer missed when CPUs are in a low power (or “sleep”) mode.	2.1(3d)B	2.2(7c)B
CSCuy01645	DIMM temperature readings are no longer not available when more than 16 degrees Centigrade different than the previous reading.	2.2(5b)B	2.2(7c)B

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCux63909	FC abort is no longer observed while running an uplink port flap test on an uplink Ethernet port-channel from an FI to a Cisco Nexus 7000 switch.	2.0(2m)B	2.2(7c)B
CSCuy34161	Any DIMM that is functioning correctly is no longer disabled after the reboot of the UCS B250 M2 blade server.	2.0(5c)B	2.2(7c)B
CSCuy62783	In a UCS setup with a VIC13xx adapter on blade servers or rack-mount servers, the server or VIC adapter no longer becomes unresponsive after running IO across network file systems.	2.2(3a)B	2.2(7c)B
CSCuy64856	The Cisco UCS fabric interconnects (FI) are no longer rebooted with the reboot reason FWM hap reset.	2.1(3h)A	2.2(7c)A
CSCuy93451	VLANs are now deleted from the vNICs if they are deleted from the updating vNIC template.	2.2(7b)A	2.2(7c)A
CSCuz69373	CATERR faults due to cpu lockup in VIC 1340 no longer occur.	2.2(7b)B	2.2(7c)B

Resolved Caveats in Release 2.2 (7b)

The following caveats are resolved in Release 2.2 (7b)

Table 19: Resolved Caveats in Release 2.2 (7b)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuz74973	When you use a B200 M4 server with a UCSB-MRAID12G SAS RAID controller and a CPLD firmware version earlier than version 05D, the B200 M4 server no longer powers off unexpectedly.	2.2(3b)B	2.2(7b)B
CSCun07367	Under normal state of operation, the statsAG process used to crash and restart on the Fabric Interconnect. This was also observed in the Cisco UCS Mini firmware. This issue has been resolved.	2.1(3a)A	2.2(7b)A 3.1(1e)A 3.1(2b)A
CSCud75506	The UUID display on ESXi 5.1 is now consistent with the UUID display on UCSM when upgrading ESXi to version 5.1 on UCS B200 M3, B22 M3 and B420 M3 blade servers.	2.0(2r)B	2.2(7b)B
CSCuv43349	During server discovery, Cisco UCS Blade server association or disassociation, the following failures are no longer reported: • `Waiting for BIOS Post Completion` • `Unable to get SCSI Device Information from the system`	2.2(6e)B	2.2(7b)B

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuw36128	The buffer overflow condition that caused the statsAG mts queue to leak is now fixed.	2.2(1d)A	2.2(7b)A
CSCuw46478	The Local disk Locator LED remains OFF, although enabled in Cisco UCS Manager.	2.2(6j)B	2.2(7b)B
CSCuw55142	Cisco UCS B420M4 server with the UCSB-MRAID12G-HE no longer reports the following critical fault: `Controller 1 on server is inoperable. Reason: Device non-responsive`	2.2(6c)B	2.2(6f)B, 2.2(7b)B
CSCux05389	After upgrading to release 2.2(7b) and rebooting the subordinate fabric interconnect, occasional VSAN misconfiguration will no longer occur.	2.2(3f)A	2.2(7b)A
CSCux07578	Cisco UCS Blade servers B400 M1 or B400 M2 running on Liberator firmware version 4.10 with SATA drives, no longer experience data consistency failures.	2.2(6f)B	2.2(7b)A
CSCux21413	When you remove and reinsert a drive in the same slot, the Locator Storage Locator LED no longer remains on all the time.	2.2(6j)B	2.2(7b)A
CSCux66675	After rebooting a Cisco UCS 6296UP FI, all physical interfaces will no longer connect incorrectly with the Cisco UCS C460 M4 servers.	2.2(6c)A	2.2(7b)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCux85580	Fabric Interconnect cores will no longer be seen on IGMP.	2.2(3b)A	2.2(7b)A
CSCux65310	During blade discovery or CIMC controller reset, a chassis thermal critical fault can be generated due to the time it takes for reconnecting from the IOM to the CIMC. However, after several minutes this fault clears on its own.	3.1(1e)B	2.2(7b)B
CSCut46044	Cisco Unified Computing Server Management Software (UCSM) includes a version of OpenSSL that is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) IDs: • CVE-2015-0286 • CVE-2015-0287 • CVE-2015-0289 • CVE-2015-0292 • CVE-2015-0293 • CVE-2015-0209 • CVE-2015-0288 This issue is now fixed.	2.2(3a)A	2.2(7b)A
CSCuw19082	During Cisco UCS Manager initial setup, while configuring the fabric interconnect, setup will assume the GUI configuration method if a DHCP lease is obtained for the mgmt interface. In addition, an url will be provided for the setup of the fabric interconnect.	2.2(6c)A	2.2(7b)A

Resolved Caveats in Release 2.2 (6j)

The following caveats are resolved in Release 2.2 (6j)

Table 20: Resolved Caveats in Release 2.2 (6j)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCux63909	FC abort is no longer observed while running an uplink port flap test on an uplink Ethernet port-channel from an FI to a Cisco Nexus 7000 switch.	2.0(2m)B	2.2(6j)B
CSCva01733	PXE in Legacy Boot mode no longer hangs with excessive unicast or multicast high background traffic with a packet size larger than MTU directed to the client server. This was seen with ESXi Autodeploy on a specific setup which likely had unusually high multicast traffic directed at the client server. This traffic was not from the PXE server for file transfer, but from some other source.	2.2(6e)B	2.2(6j)B

Resolved Caveats in Release 2.2 (6i)

The following caveats are resolved in Release 2.2 (6i)

Table 21: Resolved Caveats in Release 2.2 (6i)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuw36128	The buffer overflow condition that caused the statsAG mts queue to leak is now fixed.	2.2(1d)A	2.2(6i)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuw44595	DIMMs with correctable ECC errors are marked Inoperable or Degraded even though correctable errors do not affect normal system operation. This issue is now resolved.	2.2(3a)A	2.2(6i)A
CSCuy01645	DIMM temperature readings are no longer missed when the temperature is 16 degrees Centigrade more than the previous reading.	2.2(5b)B	2.2(6i)B
CSCuj71400	Cisco UCS Manager no longer displays the "FCoE or FC uplink is down on VSAN X" fault when the member ports for the VSAN are up.	2.2(1a)A	2.2(6i)A
CSCuy62783	In a UCS setup with a VIC13xx adapter on blade servers or rack-mount servers, the server or VIC adapter no longer becomes unresponsive after running IO across network file systems.	2.2(3a)B	2.2(6i)B
CSCuy34161	Any DIMM that is functioning correctly is no longer disabled after the reboot of the UCS B250 M2 blade server.	2.0(5c)B	2.2(6i)B
CSCux58865	DIMM temperature readings are no longer missed when the temperature is 10 degrees Centigrade more than the previous reading.	2.1(3d)B	2.2(6i)B

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuu40978	The syslog is now truncated after it reaches the configured maximum size. It no longer fills up the Fabric Interconnect file system.	2.2(3d)A	2.2(6i)A
CSCux45723	UCS SNMP memory leaks no longer occur when polling FC interfaces and SNMP processes (Walk/Get/Get Bulk) that parse any of the following SNMP MIBs: • fcIfNonLipF8Out • fcIfTimeOutDiscards • fcIfOutDiscards • fcIfCreditLoss • fcIfTxWtAvgBBCreditTransitionToZero	2.2(3a)A	2.2(6i)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuq57142	In a port channel universe, the following no longer happen: • A port channel ID may sometimes not be released after use. This could eventually lead to the universe of port channel IDs being empty, and no port channel IDs being available for use. • After an upgrade, power loss, FI reboot or failover, the empty port channel universe is incorrectly interpreted as a new installation, and repopulated. This leads to duplicate port channel ID allocation when a server is attached to the FI, or when a server is re-acknowledged.	2.2(3a)A	2.2(6i)A
CSCuw02439	When using Cisco UCS M81KR VIC adapters on a system running Cisco UCS Manager Release 2.2(2c), the adapters no longer crash and generate core files.	2.2(2c)B	2.2(6i)B
CSCux59298	When using UCS B200 M3 servers with VIC 1240 on a system running Cisco UCSM Release 2.2(2c), network and SAN no longer lose connectivity.	2.2(2c)B	2.2(6i)B

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuy64856	The Cisco UCS fabric interconnects (FI) are no longer rebooted with the reboot reason FWM hap reset.	2.1(3h)A	2.2(6i)A
CSCuz20650	When syslog messages are generated continuously, the syslog suspend timer does not recover. Thus, no events are sent to the remote syslog server. This issue is now resolved.	2.2(3a)A	2.2(6i)A
CSCuu40291	When debug logging is enabled, Cisco UCS Manager tech-support showed that syslogd_debug files were present, but the **show debug logfile syslogd_debugs** CLI command failed with the following error: `Logfile(syslogd_debugs) does not exist` This issue is now resolved.	2.2(3a)A	2.2(6i)A

Resolved Caveats in Release 2.2 (6g)

The following caveats are resolved in Release 2.2 (6g)

Table 22: Resolved Caveats in Release 2.2 (6g)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCux98751	Anytime a new blade is inserted into the chassis, or a blade CIMC controller reboots, a chassis thermal fault is no longer generated because of the time taken to reconnect from the IOM to the CIMC.	2.2(6c)B	2.2(6g)B

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuv20324	The FCoE storage no longer becomes unavailable or performs very poorly after a reset of either host-attached switch in the case of standalone systems, or after the reset of an IOM or FI in UCS-managed systems when the IOM or FI sends configuration information to the adapter later than 5 seconds after link-up.	2.2(1b)B	2.2(6g)B
CSCuv89839	When the fabric interconnect is in switch mode with direct attached storage, and its FC uplinks to the direct attached storage are up, these FC uplinks now allow traffic to pass.	2.2(3f)A	2.2(6g)A
CSCuv97713	After upgrading Cisco UCS Manager, in rare cases, the IOM may core in the sysmgr process leading to IOM reboot. This is now resolved.	2.2(3j)A	2.2(6g)A
CSCux68679	When a UCS B460 M4 server is configured with Fusion IO cards installed in same mezzanine slot of the master and slave blades, actions such as Cisco UCS Manager upgrade, cluster failover, fabric interconnect reboot no longer trigger server reboot.	2.2(3a)A	2.2(6g)A
CSCux96432	Discovery no longer fails on UCS B420 M4 servers with a 2-CPU configuration and a Fusion IO card in adapter slot 3.	2.2(5b)B	2.2(6g)B

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCux76128	Firmware Auto Install upgrade validation fails as expected when upgrading to Cisco UCS Manager Release 2.2(6g) with deprecated hardware. Auto Install can now be initiated by using the force option either through the GUI or the CLI.	2.1(3j)A	2.2(6g)A

Resolved Caveats in Release 2.2 (6f)

The following caveats are resolved in Release 2.2 (6f)

Table 23: Resolved Caveats in Release 2.2 (6f)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuv46749	When using Cisco B200 M4 blade servers with the UCSB-MRAID12G storage controller, the following random, incorrect transient alerts or faults are no longer reported: • Critical Fault [F1004] Controller Inoperable, Reason: Device reported corrupt data • Critical Fault [F1004] Controller Inoperable, Reason: Device non-responsive	2.2(3g)B	2.2(6f)B

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCux40478	When installing a Cisco B200 M3 blade server with a UCSB-MLOM-40G-01 40G VIC and either a UCSB-F-FIO-1300MP or a UCSB-F-1600MS ioMemory PCIe flash Mezzanine card, in a chassis with an N20-I6584 IOM, blade discovery no longer fails because of an “Invalid adapter-iocard combination” error.	2.2(5b)B	2.2(6f)B
CSCux47667	Service profile association no longer fails if the service profile was previously associated to a different server with LUN deployed.	2.2(6e)A	2.2(6f)A
CSCuw44524	The server reboot issues related to clear CMOS BIOS operation in Cisco UCS Manager Release 2.2(5a), 2.2(5b), 2.2(5c) or 2.2(6c) for E7 v2 processors on the C460 M4, B260 M4, and B460 M4 servers are resolved.	2.2(5a)B	2.2(6e)B
CSCuw23829	When inserting a HDD into the final disk slot of a C240 M4 server with 8 supported slots for disks, Cisco UCS Manager no longer displays a disk in the 9th slot.	2.2(4b)A	2.2(6e)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCux10203	When you decommission a C-Series server after it was discovered in direct attached configuration, and the direct attached switch port was changed from Ethernet to FC mode, the following error message no longer appears:	2.2(3h)A	2.2(3j)A, 2.2(6e)A
	Warning : if_index 0x1a01a000[Ethx/x] does not exists in VLAN database#ERROR		
CSCuw84010	Integrated C-Series rack servers with Seagate drives no longer fail association when using the host firmware policy in a service profile.	2.2(3h)A	2.2(3j)A, 2.2(6e)A
CSCuw59409	The DME crash issue that you may experience when you upgrade a directly connected C-Series rack server without decommissioning to 2.2(5c), and connect the server to FI port, is resolved.	2.2(3h)A	2.2(3j)A, 2.2(6e)A
CSCuv55823	Faults no longer occur when incompatible combinations of CIMC firmware and UCS Manager firmware are installed at the same time.	2.2(1a)A	2.2(6e)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuv32417	Cisco B200 M4 and B420 M4 blade servers that run on UEFI OS will not reboot unexpectedly. **Note** BIOS POST not being set as complete, which causes the next shallow discovery to reboot the server, has been resolved. Shallow discovery can occur because of different events including Cisco UCS Manager cluster failover, CIMC reset, or chassis reacknowledgment.	2.2(4b)B	2.2(6e)B

Resolved Caveats in Release 2.2 (6e)

The following caveats are resolved in Release 2.2 (6e)

Table 24: Resolved Caveats in Release 2.2 (6e)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuw44524	The server reboot issues related to clear CMOS BIOS operation in Cisco UCS Manager Release 2.2(5a), 2.2(5b), 2.2(5c) or 2.2(6c) for E7 v2 processors on the C460 M4, B260 M4, and B460 M4 servers are resolved.	2.2(5a)B	2.2(6e)B
CSCuw23829	When inserting a HDD into the final disk slot of a C240 M4 server with 8 supported slots for disks, Cisco UCS Manager no longer displays a disk in the 9th slot.	2.2(4b)A	2.2(6e)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCux10203	When you decommission a C-Series server after it was discovered in direct attached configuration, and the direct attached switch port was changed from Ethernet to FC mode, the following error message no longer appears:		
Warning : if_index 0x1a01a000[Ethx/x] does not exists in VLAN database#ERROR	2.2(3h)A	2.2(3j)A, 2.2(6e)A	
CSCuw84010	Integrated C-Series rack servers with Seagate drives no longer fail association when using the host firmware policy in a service profile.	2.2(3h)A	2.2(3j)A, 2.2(6e)A
CSCuw59409	The DME crash issue that you may experience when you upgrade a directly connected C-Series rack server without decommissioning to 2.2(5c), and connect the server to FI port, is resolved.	2.2(3h)A	2.2(3j)A, 2.2(6e)A
CSCuv55823	Faults no longer occur when incompatible combinations of CIMC firmware and UCS Manager firmware are installed at the same time.	2.2(1a)A	2.2(6e)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuv32417	Cisco B200 M4 and B420 M4 blade servers that run on UEFI OS will not reboot unexpectedly. **Note** BIOS POST not being set as complete, which causes the next shallow discovery to reboot the server, has been resolved. Shallow discovery can occur because of different events including Cisco UCS Manager cluster failover, CIMC reset, or chassis reacknowledgment.	2.2(4b)B	2.2(6e)B

Resolved Caveats in Release 2.2 (6d)

The following caveats are resolved in Release 2.2 (6d)

Table 25: Resolved Caveats in Release 2.2 (6d)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuv45173	When you upgrade C-series server firmware for C220-M4, C240-M4 to Cisco UCS Manager 2.2(6d), you will no longer see the following critical alarm: Board controller upgraded, manual a/c power cycle required on server x.	2.2(6d)	2.2(6d)C

Resolved Caveats in Release 2.2 (6c)

The following caveats are resolved in Release 2.2 (6c)

Table 26: Resolved Caveats in Release 2.2 (6c)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuq77241	Inventory scanning software such as Snow Inventory on Windows OS, CIMC, host OS or a remote KVM session no longer goes into an unresponsive state.	2.2(2c)B	2.2(6c)B
CSCuw03000	PXE boot fails with BSOD when RoCE is enabled.	2.2(5a)B	2.2(6c)B
CSCut78943	When making changes to vNICs or vHBAs that will be provisioned on Cisco Virtual Interface Cards (VICs) 1340 and 1380 adapters, a warning on the placement order impact appears.	2.2(3c)A	2.2(6c)A
CSCuu33864	When upgrading to UCS Manager 2.2(6c) or later, the FI boots successfully without the possibility of causing a file system corruption on the SSD if the FI is equipped with a Unigen SSD.	2.2(3b)A	2.2(6c)A, 3.1(1e), 3.1(2b)
CSCum50468	After upgrading the UCS Manager to version 2.2(6c) or higher, false faults for Fabric VSAN Membership Down are cleared.	2.2(1b)A	2.2(6c)A
CSCut37134	A Cisco UCS B200 M4 server running ESXi 5.5 no longer crashes when you boot locally.	2.2(3a)A	2.2(6c)A
CSCur79257	During an FI bootup, the RACE condition no longer causes UCS Manager configure interface vethernet 0” to switch.	2.2(3a)A	2.2(6c)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCup95855	FSM tasks are no longer stuck in the throttled state in Cisco UCS Manager during Cisco UCS C240 M3 server upgrade.	2.2(1d)A	2.2(3j)A, 2.2(6c)A
CSCuv51214	Messages log are no longer overfilled with BMC is suspecting that palo is in the boot block. Leaving I2C bus alone messages.	2.2(3g)B	2.2(6c)B
CSCuo93591	For a fabric interconnect in end-host mode, the MAC address table aging time no longer gets stuck at 300 regardless of the configuration. The value got stuck at 300 regardless of the configuration. This was the issue which was resolved. This value can be changed through UCSM GUI or CLI.	2.2(1c)A	2.2(6c)A
CSCuu68351	The updated BIOS in UCS M3 B-Series Servers is compatible when running the Snow Inventory client on Windows OS, and does not hang.	2.0(1m)B	2.2(6c)B
CSCut88909	The KVM option, Virtual Media > Activate Virtual Devices is now available.	2.2(3b)A	2.2(6c)A
CSCuu55899	When the VLAN port-count optimization is enabled, and an uplink Ethernet is in a port channel, traffic is now able to flow to the available members in the port channel when there is a link flap on one of its members.	2.2(3b)A	2.2(6c)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuq63868	When creating a vNIC in a LAN connectivity policy, the show configuration command no longer generates a software error.	2.2(2a)A	2.2(6c)A
CSCut35123	After high-availability failover, chassis-seeprom local IO failures are no longer triggered.	2.2(4b)A	2.2(6c)A

Resolved Caveats in Release 2.2 (5d)

The following caveats are resolved in Release 2.2 (5d)

Table 27: Resolved Caveats in Release 2.2 (5d)

Defect ID	Description	First Bundle Affected	Resolved in Release

CSCuw50417	After upgrading the BIOS of Cisco UCS B200 M3 servers to Release 2.2(5d), the OS no longer displays the following error message if the OS boot time is exceptionally slow:
	`Initializing Power Management ...`
	`Power: 2568: No supported CPU power management technology detected`
	`Intel Enhanced SpeedStep is supported but disabled in BIOS`
		2.2(4b)B	2.2(5d)B

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuv20999	When Cisco UCS Manager is managed by Cisco UCS Central, and there is a global service profile associated with a blade server, global VLANs can now be successfully assigned to a particular uplink interface through Cisco UCS Manager (VLAN Uplink Manager > VLANs > VLAN Manager) without an error message being displayed.	2.2(4b)A	2.2(5d)A
CSCuw13170	When auto-deploying the installation of ESX on Ivy Bridge-EX platforms, some platforms that enforce ACS violations strictly will no longer generate a non-maskable interrupt (NMI) and crash the host OS.	2.2(5c)B	2.2(5d)B

Resolved Caveats in Release 2.2 (5c)

The following caveats are resolved in Release 2.2 (5c)

Table 28: Resolved Caveats in Release 2.2 (5c)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuu89283	You can create LUNs with certain non-default virtual drive policy attributes, such as read-policy, write-policy, and cache-policy, which are managed through storage profiles for rack servers with a UCSC-MRAID12G storage controller. You can modify such virtual drive policy attributes for these LUNs as well without causing service profile association to fail.	2.2(4b)A	2.2(5c)A
CSCuv00089	After upgrading the Fabric Interconnect (FI) to Cisco UCS Manager Release 2.2(5c), systems that have OS-based NIC teaming configured as Active-Standby no longer experience network connectivity issues. **Note** Network connectivity issues still occur on systems that have OS-based NIC teaming configured as Active-Standby when you upgrade the FI to Cisco UCS Manager Release 2.2(4).	2.2(4b)A	2.2(5c)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuv49345	When a server is discovered from only one Fabric Interconnect (FI), and the DME primary instance is the other FI, disassociation of the associated service profile no longer fails.	2.2(1a)A	2.2(5c)A
CSCuu60867	Cisco UCS C240 M3 servers with dual RAID controllers can now be discovered on SimpliVity solutions with OmniStack cards.	2.2(3f)A	2.2(5c)A
CSCuv13545	If Cisco UCS Manager is registered with Cisco UCS Central, and the service profile refers to a global host firmware pack policy, UCSM no longer downloads images during shallow discovery.	2.2(4b)A	2.2(5c)A
CSCuv28540	When you run Cisco UCS Manager Releases between 2.2(1) and 2.2(3) with catalog version 2.2(5b)T, the VIC PCI slot ID is now populated correctly. Hence, SAN boot no longer fails on servers where the boot vHBAs are placed on a VIC. **Note** This issue still occurs when you run UCSM Releases between 2.2(1) and 2.2(3) with catalog versions 2.2(4b)T and 2.2(5a)T.	2.2(4b)T	2.2(5b)T

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuu15250	Toggling the locator LED for a Fabric Interconnect in UCSM no longer fails.	2.2(1d)A	2.2(5c)A

Resolved Caveats in Release 2.2 (5b)

The following caveats are resolved in Release 2.2 (5b)

Table 29: Resolved Caveats in Release 2.2 (5b)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuv04436	Cisco UCS B200 M4 servers with the following CPUs will no longer experience performance degradation: • E5-2667 v3 • E5-2643 v3 • E5-2640 v3 • E5-2637 v3 • E5-2630 v3 • E5-2630L v3 • E5-2623 v3 • E5-2620 v3 • E5-2609 v3	2.2(4b)B	2.2(5b)B 2.2(4c)B
CSCuv29668	When using Cisco UCS 6100 Series Fabric Interconnects with Cisco UCS 2100 IOMs, blade servers with two Cisco UCS M81KR VIC adapters no longer fail discovery after updating Cisco UCS Manager to Release 2.2.(5b) and later releases.	2.2(4b)A	2.2(5b)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCus11782	After rebooting a Cisco UCS 6248UP Fabric Interconnect (FI) that is operating in the FC end-host mode, all member links of the SAN port channel come up.	2.2(1d)A	2.2(3j)A, 2.2(5b)A
CSCuu35687	In Cisco UCS B420 M4 servers with UCSB-MRAID12G and UCSB-LSTOR-PT RAID controllers, the Fault/Locator LEDs for disks 3 and 4 are no longer swapped.	2.2(5a)B	2.2(5b)B
CSCuu58282	In Cisco UCS B420 M4 servers with UCSB-MRAID12G and UCSB-LSTOR-PT RAID controllers, in the rare event that Online Controller Reset (OCR) is triggered during normal I/Os on JBOD drives, excessive Fast Path IO failures are no longer seen after the controller is reset.	2.2(5a)B	2.2(5b)B

Resolved Caveats in Release 2.2 (5a)

The following caveats are resolved in Release 2.2 (5a)

Table 30: Resolved Caveats in Release 2.2 (5a)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCus03683	The Cisco UCS 6200 series primary and subordinate FIs no longer reboot unexpectedly due to high volume traffic impacting the management interface.	2.2(1d)A	2.2(5a)A, 2.2(4b)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCut54652	During service profile association, firmware upgrade on third-party Converged Network Adapters (CNA) no longer fails with the following error: `Unable to find VNIC Device`	2.2(4b)A	2.2(5a)A
CSCuu37369	Storage profiles can now be created within a sub-organization in Cisco UCS Manager.	2.2(4b)A	2.2(5a)A
CSCuu42945	Service profiles created from service profile templates with local storage profiles no longer fail association with server pools.	2.2(4b)A	2.2(5a)A
CSCuu52001	In Cisco UCS C240 M3 rack mount servers with external LSI RAID controllers, service profile association no longer fails.	2.2(4b)A	2.2(5a)A
CSCuu53920	In Cisco UCS B260 M4 and B 460 M4 servers, LUN creation and service profile association no longer fails.	2.2(4b)A	2.2(5a)A
CSCuu65128	Continuous reboots of Cisco UCS 6200 series Fabric Interconnect are no longer observed after configuring more than 64 vNICs (excluding dynamic vNICs) on a single server.	2.2(4b)A	2.2(5a)A

Resolved Caveats in Release 2.2 (4c)

The following caveats are resolved in Release 2.2 (4c)

Table 31: Resolved Caveats in Release 2.2 (4c)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuv04436	Cisco UCS B200 M4 servers with the following CPUs will no longer experience performance degradation: • E5-2667 v3 • E5-2643 v3 • E5-2640 v3 • E5-2637 v3 • E5-2630 v3 • E5-2630L v3 • E5-2623 v3 • E5-2620 v3 • E5-2609 v3	2.2(4b)B	2.2(4c)B

Resolved Caveats in Release 2.2 (4b)

The following caveats are resolved in Release 2.2 (4b)

Table 32: Resolved Caveats in Release 2.2 (4b)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCus03683	The Cisco UCS 6200 series primary and subordinate FIs no longer reboot unexpectedly due to high volume traffic impacting the management interface.	2.2(1d)A	2.2(4b)A, 2.2(5a)A
CSCus81832	Using a Cisco UCS VIC 1340 or VIC 1380 adapter with a Sandy Bridge CPU in a Cisco UCS B420 or UCS B200 M3 server no longer causes the server to hang. Red Hat Enterprise Linux 6.5 or 7.0 now installs successfully.	2.2(3c)B	2.2(4b)B

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCus18092	IOMs that are connected to a Fabric Interconnect no longer reboot due to a software-controlled reset.	2.1(3e)A	2.2(4b)A
CSCus10255	The number of licenses used by ports is now displayed correctly.	2.2(3a)A	2.2(4b)A, 2.2(6c)A
CSCup88161	Cisco UCS 6248 Fabric Interconnect crashes with no cores are no longer observed when new blade servers are being added to the environment.	2.2 (1d)A	2.2(4b)A
CSCus72177	After changing the IP address of the KVM pool and Fabric Interconnect from one subnet to another, KVM launches successfully.	2.2(3d)A	2.2(4b)A
CSCus40519	Changing the Fibre Channel trunking mode when the Fibre Channel port-channel is active no longer impacts the Fabric Interconnect expansion module.	2.2(3c)A	2.2(4b)A
CSCur39162	When you run the **show platform fwm info hw-stm asic num** command on a Fabric Interconnect, the FWM process no longer crashes and reboots the Fabric Interconnect.	2.0(1q)A	2.2(4b)A
CSCup99955	In a scale Cisco UCS environment, the Call Home process no longer crashes and reboots the Fabric Interconnect due to a memory leak.	2.2(1b)A	2.2(4b)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCut04941	Cisco UCS clusters scheduled for an update from Cisco UCS Central will conform to the user acknowledgment setting.	2.2(1b)A	2.2(4b)A
CSCur79565	On a Cisco UCS B-Series server running Cisco UCS Manager Release 2.2(3b) or later versions, Netflow data is now sent to the collector.	2.2(3b)A	2.2(4b)A
CSCut03052	IP QoS core may happen in a VM-FEX scale set up, when you reboot Fabric Interconnects back to back.	2.2(1b)A	2.2(4b)A
CSCva43666	Whenever the chassis IOM is reset, the FI server port no longer gets into Error disable state.	2.2(3a)A	2.2(4b)A

Resolved Caveats in Release 2.2 (3l)

The following caveats are resolved in Release 2.2 (3l)

Table 33: Resolved Caveats in Release 2.2 (3l)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuu66595	It is now possible to perform multiple backups to the same host.	2.2(3f)A	2.2(3l)A
CSCuu99255	The “show fabric-interconnect inventory expand” command no longer displays the ethernet port with a role of “Unknown” instead of “Server” on a fabric interconnect with a GEM card.	2.1(1a)A	2.2(3l)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuw78008	Web sessions no longer remain on after the Web Session Timeout period specified in the authentication option under user management in the Admin tab.	2.1(3a)A	2.2(3l)A
CSCuz55693	When you attempt to reset memory errors using **ucs-fi chassis/server #** **reset-all-memory-errors** Cisco UCS Manager no longer generates a 'Managed object does not exist' error.	2.2(1b)A	2.2(3l)A
CSCuz86450	The server no longer reboots because the system does not accept user input on the order property of adaptorHostIf.	1.4(1j)A	2.2(3l)A
CSCvb78971	When attempting the auto-install of UCS Manager, the fabric interconnect upgrade no longer fails when the /var/tmp usage exceeds 10%.	2.1(3k)A	2.2(3l)A
CSCvb85544	A race condition in the Linux kernel's memory subsystem that handled the copy-on-write (COW) of read-only memory mappings no longer occurs on fabric interconnects. This vulnerability is documented in Common Vulnerability and Exposures (CVE) CVE-2016-5195.	2.2(1a)A	2.2(3l)A

Resolved Caveats in Release 2.2 (3k)

The following caveats are resolved in Release 2.2 (3k)

Table 34: Resolved Caveats in Release 2.2 (3k)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuv03557	During Cisco UCS Manager upgrade, FI activation no longer fails with the following error: `Pre-Upgrade check failed. Insufficient free space in /var/tmp. Less than required 90%.`	2.1(3a)A	2.2(3k)A
CSCuv46749	When using Cisco B200 M4 blade servers with the UCSB-MRAID12G storage controller, the following random, incorrect transient alerts or faults are no longer reported: • Critical Fault [F1004] Controller Inoperable, Reason: Device reported • Critical Fault [F1004] Controller Inoperable, Reason: Device non-responsive	2.2(3g)B	2.2(3k)B
CSCuv53399	After IOM firmware upgrade, or after an IOM reset while running effected firmware, Cisco UCS Manager will no longer show Major fault F0481 indicating the IOM encountered a POST failure.	2.2(3a)A	2.2(3k)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuv89839	When the fabric interconnect is in switch mode with direct attached storage, and its FC uplinks to the direct attached storage are up, these FC uplinks now allow traffic to pass.	2.2(3f)A	2.2(3k)A
CSCuv97713	After upgrading Cisco UCS Manager, in rare cases, the IOM may core in the sysmgr process leading to IOM reboot. This is now resolved.	2.2(3j)A	2.2(3k)A
CSCuj71400	Cisco UCS Manager no longer displays the ’FCoE or FC uplink is down on VSAN X' fault when the member ports for the VSAN are up.	2.2(1a)A	2.2(3k)A
CSCuo93591	For a fabric interconnect in end-host mode, the MAC address table aging time no longer gets stuck at 300 regardless of the configuration. The value got stuck at 300 regardless of the configuration. This issue in now resolved. This value can be changed through UCSM GUI or CLI.	2.2(1c)A	2.2(3k)A
CSCus34689	When using Cisco UCS Manager with C-Series integration, Cisco UCSM GUI no longer displays the following message on hovering between the C-Series servers and FIs:	2.2(1b)A	2.2(3k)A
CSCuw36128	The buffer overflow condition that caused the statsAG mts queue to leak is now fixed.	2.2(1d)A	2.2(3k)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuw44595	DIMMs with correctable ECC errors are marked Inoperable or Degraded even though correctable errors do not affect normal system operation. This issue is now resolved.	2.2(3a)A	2.2(3k)A
CSCur39162	When you run the show platform **fwm info hw-stm asic num** command on a Fabric Interconnect, the FWM process no longer crashes and reboots the Fabric Interconnect.	2.0(1q)A	2.2(3k)A
CSCus59926	You can see the following issues with Call Home messages, although Smart Call Home registers successfully: • Call Home messages are not generated. • Test inventory is not sent. This issue is now resolved.	2.2(3a)A	2.2(3k)A
CSCus76125	Global service profile now resolves the LAN ping group even when the ping group is created in Cisco UCS Manager.	2.2(3d)A	2.2(3k)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuv20324	The FCoE storage no longer becomes unavailable or performs very poorly after a reset of either host-attached switch in the case of standalone systems, or after the reset of an IOM or FI in UCS-managed systems when the IOM or FI sends configuration information to the adapter later than 5 seconds after link-up.	2.2(1b)B	2.2(3k)A
CSCux68679	When a UCS B460 M4 server is configured with Fusion IO cards installed in same mezzanine slot of the master and slave blades, actions such as Cisco UCS Manager upgrade, cluster failover, fabric interconnect reboot no longer trigger server reboot.	2.2(3a)A	2.2(3k)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuq57142	In a port channel universe, the following no longer happen: • A port channel ID may sometimes not be released after use. This could eventually lead to the universe of port channel IDs being empty, and no port channel IDs being available for use. • After an upgrade, power loss, FI reboot or failover, the empty port channel universe is incorrectly interpreted as a new installation, and repopulated. This leads to duplicate port channel ID allocation when a server is attached to the FI, or when a server is re-acknowledged.	2.2(3a)A	2.2(3k)A
CSCux45723	UCS SNMP memory leaks no longer occur when polling FC interfaces and SNMP processes (Walk/Get/Get Bulk) that parse any of the following SNMP MIBs: • fcIfNonLipF8Out • fcIfTimeOutDiscards • fcIfOutDiscards • fcIfCreditLoss • fcIfTxWtAvgBBCreditTransitionToZero	2.2(3a)A	2.2(3k)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCux59298	When using UCS B200 M3 servers with VIC 1240 on a system running Cisco UCSM Release 2.2(2c), network and SAN no longer lose connectivity.	2.2(2c)B	2.2(3k)A
CSCuy64856	The Cisco UCS fabric interconnects (FI) are no longer rebooted with the reboot reason FWM hap reset.	2.1(3h)A	2.2(3k)A
CSCuu40291	When debug logging is enabled, Cisco UCS Manager tech-support showed that syslogd_debug files were present, but the show debug **logfile syslogd_debugs** CLI command failed with the following error: `Logfile(syslogd_debugs) does not exist` This issue is now resolved.	2.2(3a)A	2.2(3k)A
CSCuu40978	The syslog is now truncated after it reaches the configured maximum size. It no longer fills up the Fabric Interconnect file system.	2.2(3d)A	2.2(3k)A
CSCuw02439	When using Cisco UCS M81KR VIC adapters on a system running Cisco UCS Manager Release 2.2(2c), the adapters no longer crash and generate core files.	2.2(2c)B	2.2(3k)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuw44595	DIMMs with correctable ECC errors are marked Inoperable or Degraded even though correctable errors do not affect normal system operation. This issue is now resolved.	2.2(3a)A	2.2(3k)A
CSCux58865	DIMM temperature readings are no longer missed when the temperature is 10 degrees Centigrade more than the previous reading.	2.1(3d)B	2.2(3k)A
CSCuz20650	When syslog messages are generated continuously, the syslog suspend timer does not recover. Thus, no events are sent to the remote syslog server. This issue is now resolved.	2.2(3a)A	2.2(3k)A
CSCuy34161	Any DIMM that is functioning correctly is no longer disabled after the reboot of the UCS B250 M2 blade server.	2.0(5c)B	2.2(3k)A

Resolved Caveats in Release 2.2 (3j)

The following caveats are resolved in Release 2.2 (3j)

Table 35: Resolved Caveats in Release 2.2 (3j)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCus55944	While updating a service profile template, the service profile no longer reboots without a warning when you create and add a VLAN to a rack server that is associated with an inherited service profile.	2.2(3a)A	2.2(3j)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuw78688	The failure to load configuration that caused system outage when upgrading Cisco UCS Manager to 2.2(5c) is resolved.	2.2(3a)A	2.2(3j)A
CSCus11782	After rebooting a Cisco UCS 6248UP Fabric Interconnect (FI) that is operating in the FC end-host mode, all member links of the SAN port channel come up.	2.2(1d)A	2.2(3j)A, 2.2(5b)A
CSCus85186	After activating Cisco Trusted Platform Module (TPM), the enable and active statuses now remain as disabled and deactivated.	2.2(1d)B	2.2(1h)B,2.2(3j)B
CSCuv06504	The svc_sam_dme process is no longer crashing during a steady state of operation when a database (db) corruption is detected primarily on the subordinate fabric interconnect.	2.2(3d)A	2.2(3j)A, 2.2(6c)A
CSCuv72975	When upgrading the Cisco UCS Manager infrastructure bundle and using VIC-1340 or VIC-1380, the backplane port of the IOM and VIC is no longer down.	2.2(3a)B	2.2(3j)B
CSCuw59409	The DME crash issue that you may experience when you upgrade a directly connected C-Series rack server without decommissioning, and connect the server to FI port, is resolved.	2.2(3h)A	2.2(3j)A, 2.2(6e)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuw84010	Integrated C-Series rack servers with Seagate drives no longer fail association when using the host firmware policy in a service profile.	2.2(3h)A	2.2(3j)A, 2.2(6e)A
CSCux10203	When you decommission a C-Series server after it was discovered in direct attached configuration, and the direct attached switch port was changed from Ethernet to FC mode, the following error message no longer appears: `Warning : if_index 0x1a01a000[Ethx/x] does not exists in VLAN database#ERROR`	2.2(3h)A	2.2(3j)A, 2.2(6e)A
CSCup95855	FSM tasks are no longer stuck in the throttled state in Cisco UCS Manager during Cisco UCS C240 M3 server upgrade.	2.2(1d)A	2.2(3j)A, 2.2(6c)A
CSCur01185	The HA policy of Reset is no longer triggering the Cisco UCS 6296UP fabric interconnect to reset.	2.2(1d)A	2.2(3j)A
CSCus32933	Cisco UCS Manager now displays an error message when a WILL_BOOT_FAULT event is raised because of an incorrect CPLD version.	2.2(2c)B	2.2(3j)B

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCus56140	Cisco UCS Manager now performs a successful failover if the primary out-of-band management port is detected as down for more than the Management Interface Monitoring default 5 minutes.	1.4(2b)A	2.2(3j)A
CSCus73964	When you download an infrastructure software bundle onto a system where the same infrastructure software bundle was previously installed, but was subsequently deleted, the UCS Manager FIs, and IOMs no longer downgrade to that software bundle.	2.1(3e)A	2.2(3j)A
CSCus93431	Adding other storage, such as a local disk or a USB to a SAN boot policy no longer deletes the SAN boot policy from Cisco UCS Manager.	2.2(3c)A	2.2(3j)A, 2.2(6c)A
CSCut10525	The FlexFlash firmware version is now updating and the FFCH_ERROR_OLD_FIRMWARE_RUNNING is not longer displaying in the fault summary after you update the UCS B200 M4 server firmware using 2.2(4b).	2.2(3a)B	2.2(3j)B
CSCut28278	After upgrading the infrastructure and the Cisco UCS Manager image, the subordinate fabric interconnect no longer fails the pre-upgrade check because of insufficient free space in the /var/sysmgr directory.	2.2(1d)A	2.2(3j)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuv31912	UCS Manager iptables are no longer duplicating rules in the FORWARD table.	2.2(3d)A	2.2(3j)A, 2.2(6c)A, 2.2(8a)A
CSCux71937	The CPU utilization always displayed 100 percent for the kernel in the output of the show system resources command. This could happen if the system had been up for a very long time (more than 200 days, but this time-frame could vary): `FI(nx-os)# show system resourcesLoad average: 1 minute: 0.50 5 minutes: 0.71 15 minutes: 1.04Processes : 563 total, 3 runningCPU states : 0.0% user, 100.0% kernel, 0.0% idleMemory usage: 3490164K total, 3140304K used, 349860K free` This has now been resolved. The output of this command now indicates the correct CPU utilization levels.	2.2(3b)A	2.2(3j)A, 2.2(6f)A

Resolved Caveats in Release 2.2 (3h)

The following caveats are resolved in Release 2.2 (3h)

Table 36: Resolved Caveats in Release 2.2 (3h)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCus64439	Cisco UCS Manager Mezz logs and VMware vmkernel logs no longer indicate storage latency and numerous FNIC aborts.	2.2(1d)B	2.2(3h)B
CSCuu15465	If the version of board controller on a UCS B200 M4 server is higher than the version in the Host Firmware Pack, Cisco UCS Manager no longer tries to downgrade firmware of board controllers on the servers. While running Cisco UCS Manager Releases 2.2(3b) to 2.2(3g), you can use catalog version 2.2(4b)T or later versions to get this fix.	2.2(3b)A	2.2(3h)A

Resolved Caveats in Release 2.2 (3g)

The following caveats are resolved in Release 2.2 (3g)

Table 37: Resolved Caveats in Release 2.2 (3g)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCus74206	After disconnecting and re-connecting a cable between the FI and IOM, the VFC interfaces on the chassis will not flap and cause any disruption in the FC traffic.	2.2(1d)A	2.2(3g)A
CSCur66094	Servers will not be stuck in discovery state. The locked CIMC connection issue causing bladeAG network thread lock up is resolved.	2.2(2c)A	2.2(3g)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCur96296	FEX will not be online and offline in quick succession under scaled setups.	2.2(3a)A	2.2(3g)A
CSCus91342	You will not be prompted to reboot the blade server when adding a vLAN to a vNIC template.	2.2(1b)A	2.2(3g)A
CSCut28626	When you import a backup file with multiple vLANs, the B200 M2 server association will not be stuck at 86%.	2.2(3e)A	2.2(3g)A
CSCut45598	6296 FI will not reboot with kernel panic.	2.2(3c)A	2.2(3g)A
CSCut54264	Server connectivity issue relative to non-reuse of connection slots is resolved. **Note** The logs will show MCSERVER_LIMIT_REACHEDIN whereas netstat will show that there are only a few connections.	2.2(1c)B	2.2(3g)B
CSCur19358	The firmware update on K2 NVIDIA adapter will not fail with the error message “FI unreachable”.	2.2(2e)	2.2(3g)A
CSCut13146	Chassis Discovery and service profile association no longer fail during downgrade to a UCSM version 2.2(2x) or earlier, when isolated Vlans are allowed on appliance ports or vNIC service profiles.	2.2(1g)A	2.2(3g)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCut61527 and CSCus42584	The Cisco B200M4 blade server will not reboot unexpectedly. **Note** Storage Controller FRU information mismatch that causes the next shallow discovery to be converted to a deep discovery has been resolved. Shallow discovery can occur through different activities such as replacing IOM cables.	2.2(3a) and 2.2(1b)A	2.2(3g)A
CSCus89837	The excessive logging of the error "error:Invalid argument" in chassis pwrmgr tech support log will not happen anymore.	2.1(3b)A	2.2(3g)A
CSCut45721	FI running BladeAG will no longer need rebooting due to low kernel memory	2.1(1a)A	2.2(3g)A
CSCus97608	Faults in Cisco UCS Manager such as "error accessing shared-storage" and timeout/failover warning within the "show cluster extended-state" are no longer displayed when several devices in several chassis are reporting EBUSY within the I2C logs.	2.2(3b)B	2.2(3g)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCut02769	dbsync between Cisco UCS Fabric Interconnects will share only the required files and will not fail when copying the files from peer FI /opt/db/flash.	2.2(3b)A	2.2(3g)A
CSCur21496	After a successful firmware update, the NVIDIA GPU cards no longer display the incorrect version number.	2.2(2e)A	2.2(3g)A
CSCur83866	All overlapping IP addresses are appropriately removed during deletion and deployed at creation.	2.2(1b)A	2.2(3g)A
CSCut69252	Service profile disassociation no longer fails with the flexflash scrub policy with no SD cards on C220 M4 servers.	2.2(3c)A	2.2(3g)A

Resolved Caveats in Release 2.2 (3f)

The following caveats are resolved in Release 2.2 (3f)

Table 38: Resolved Caveats in Release 2.2 (3f)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCus61659	After an IOM is reset, priority flow control on the IOM interface to a blade no longer becomes disabled.	2.1(3c)A	2.2(3f)A
CSCuq95926	Fabric Interconnect failover status is no longer stuck in Switchover In Progress when the management cable is unplugged.	2.2(2c)A	2.2(3f)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCut11027	When using a maintenance policy with user acknowledgment, a server with a third-party adapter will not reboot without asking for user acknowledgment after a SAN boot change in the boot policy.	2.2(3c)A	2.2(3f)A
CSCuq51890	Entity physical description returns correct getnext values during SNMPwalk on Entity MIB.	2.2(2c)A	2.2(3f)A

Resolved Caveats in Release 2.2 (3e)

The following caveats are resolved in Release 2.2 (3e)

Table 39: Resolved Caveats in Release 2.2 (3e)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCus69458	The heap-based buffer overflow vulnerability in the GNU C library, documented in Common Vulnerability and Exposures (CVE) CVE-2015-0235 is addressed.	1.0(1e)	2.2(3e)A
CSCur70034	Service Profiles with a common VLAN name configured on one of the vNICs no longer fail with the following error: “Incorrect VLAN configuration on one of the VNICs.	2.2(3c)A	2.2(3e)A
CSCuh78503	iSCSI reboot loop no longer fails with Oprom initialize error 1.	2.1(2a)B	2.2(3e)B
CSCur83235	KVM login no longer fails in UCS Manager Release 2.2(3e) over Cisco AnyConnect VPN.	2.2(2c)A	2.2(3e)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCus55072	When C460-M4 servers are unassociated, firmware upgrade FSM no longer restarts after the BIOS POST FSM stage.	2.2(3a)A	2.2(3e)A
CSCus51733	Toshiba HDD firmware version 5706 is now packaged in UCS Manager. Downgrades to version 5705 can change the status of the Toshiba HDD to Unconfigured Bad and should be avoided.	2.2(3a)B	2.2(3e)B
CSCur99740	Fabric Interconnect image upgrade no longer fails when you run the reload all command from the Fabric Interconnect.	2.2(3d)A	2.2(3e)A

Resolved Caveats in Release 2.2 (3d)

The following caveats are resolved in Release 2.2 (3d)

Table 40: Resolved Caveats in Release 2.2 (3d)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCur32075	The following new microcode for the Haswell-EP processor was added to release 2.2(3d): • M6F306F2_0000002B	2.2(3a)B	2.2(3d)B
CSCur42086	Blade AG no longer cores constantly and prevents assigning a service profile.	2.2(1d)A	2.2(3d)A
CSCur77716	Call Home Config FSM error no longer occurs when upgrading from 2.2(1f).	2.2(3c)A	2.2(3d)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuq17289	‘Failed to allocate exchange’ messages are no longer observed when vNICS with different COS values are used.	2.2(3c)A	2.2(3d)A
CSCuq74472	Unnecessary thermal events on IOM stating that the thermal sensor reading is not available no longer occur.	2.1(3c)A	2.2(3d)A
CSCur05013	Messages.log file on a Cisco UCS B200 M2 blade no longer fills with messages including ‘364:BMC lost control of the bus.[0xd 0x0]’.	2.2(2c)B	2.2(3d)B
CSCur29264	The security vulnerability identified by Common Vulnerability and Exposures (CVE) CVE-2014-3566 is addressed.	2.2(3a)A	2.2(3d)A
CSCur38408	Fabric interconnect HA failover no longer causes the attached Cisco UCS C460 M4 servers to reboot when a PCIe card is present in slot 2 and riser 2 is missing.	2.2(2c)A	2.2(3d)A
CSCur48661	Global service profile association no longer fails with a ‘failed to copy images’ error.	2.2(3b)A	2.2(3d)A
CSCun23603	UCS Manager now properly upgrades the power sequencer software.	2.2(3c)A	2.2(3d)A
CSCur37260	FI upgrade or downgrade no longer fails due to lack of disk space in /mnt/pss.	2.1(3b)A	2.2(3d)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuq52499	Cisco UCS Manager no longer raises a unnecessary fault on the IOM when the CPU on a blade in the chassis crosses the UNC/UC threshold.	2.1(3b)A	2.2(3d)A

Resolved Caveats in Release 2.2 (3c)

The following caveats are resolved in Release 2.2 (3c)

Table 41: Resolved Caveats in Release 2.2 (3c)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuq35685	IGMPv2 traffic no longer causes MAC flapping on upstream switches when the FI has multiple uplinks connecting to different switches.	2.2(1b)A	2.2(3c)A
CSCuq46105	UCS Manager now uses power sequencer version 3.0 to address the rare issue of an unexpected reboot to the Cisco UCS 6248 FI.	2.2(1c)A	2.2(3c)A
CSCuq63086	Cisco B200 M3 no longer fails with a ‘Controller 1 on server x/y is inoperable’ error.	2.2(1e)B	2.2(3c)B
CSCur08722	Firmware upgrade FSM no longer fails on the Cisco UCS C240 M3 server with the following error: `IVY Bridge Processor is installed on this server, cannot downgrade to unsupported CIMC version.`	2.2(3a)A	2.2(3c)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCup45930	When upgrading the Cisco UCS B230 M2 server from Cisco UCS Manager Release 2.2(1x) to Cisco UCS Manager Release 2.2(2x) or from Cisco UCS Manager Release 2.2(2x) to Cisco UCS Manager Release 2.2(3x), or when upgrading the Cisco UCS C460 M4 server from Cisco UCS Manager Release 2.2(2x) to Cisco UCS Manager Release 2.2(3x), association no longer fails.	2.2(1e)A	2.2(3c)A

Resolved Caveats in Release 2.2 (3b)

The following caveats are resolved in Release 2.2 (3b)

Table 42: Resolved Caveats in Release 2.2 (3b)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuq63592	Blade association no longer fails on servers with Cisco UCS VIC 1340 or VIC 1380 adapters when some vHBAs manually configured in the service profile on Host Port 1 or Host Port 2 while other vHBAs are placed systematically by setting **Desired Host Port** to ‘ANY.’	2.2(3a)A	2.2(3b)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuq64931	Blades with Cisco UCS VIC 1340 or VIC 1380 adapters no longer fail to PXE boot / iSCSI boot/ SAN boot when SRIOV vNICs (PF and VF) are placed on first host port and PXE vNIC/ iSCSI vNIC / SAN boot vHBA are placed on second host port.	2.2(3a)A	2.2(3b)A
CSCuq70724	DIMM I2C controller is automatically reset if there are invalid I2C transactions that prevent the chassis from obtaining temperature readings from blades (which can cause fan speeds to spin at 100%).	2.2(2d)B	2.2(3b)B
CSCuq81262	Cisco UCS Manager no longer becomes unresponsive (after seven days when VM-related data collection begins) if anonymous reporting (AR) is enabled when upgrading to Cisco UCS Manager release 2.2(3b) in an environment specifically configured with VMs that use VM-FEX on any hypervisor.	2.2(3a)A	2.2(3b)A
CSCuq92477	Infra bundle upgrades from Cisco UCS Manager release 2.2(3a) no longer fail if performed from Cisco UCS Central.	2.2(3a)A	2.2(3b)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCur01379	The security vulnerabilities identified by Common Vulnerability and Exposures (CVE) CVE-2014-7169, CVE-2014-6271, CVE-2014-6277, CVE-2014-7186, CVE-2014-7187, and CVE-2014-6278 are addressed.	2.0(1q)A	2.2(3b)A

Resolved Caveats in Release 2.2 (3a)

The following caveats are resolved in Release 2.2 (3a)

Table 43: Resolved Caveats in Release 2.2 (3a)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuo60330	IOMs are no longer unreachable after upgrading the FI when upgrading to Cisco UCS Manager, Release 2.2(2) or later.	2.2(1d)A	2.2(3a)A
CSCue93518	Cisco UCS Manager now displays an alert when users are close to reaching the VLAN port count limit.	2.1(1a)A	2.2(3a)A
CSCug73260	The UCS Manager DME process no longer crashes on the subordinate FI during an upgrade or power outage.	2.1(1a)A	2.2(3a)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCui12868	Some conditions that result in the chassis displaying a thermal sensor reading error due to third-party applications accessing the PCH SMBus or CPU SMBus controller have been fixed. **Note** An additional enhancement addressing this same symptom will be included in the upcoming 2.2(3b) patch.	2.0(4b)B	2.2(3a)B
CSCui53234	Call Home alerts now include alert customization and service profile information.	2.0(3a)A	2.2(3a)A
CSCul69513	Interface (error) counters for the fabric ports on the IOM can now be monitored using the UCS Manager GUI and CLI.	2.1(1a)A	2.2(3a)A
CSCum48026	Local vMedia mounts in progress can now be cancelled by the user instead of waiting for a timeout.	2.2(2c)B	2.2(3a)B
CSCun00368	A fault is now raised if the FI has less memory than expected.	2.1(3b)A	2.2(3a)A
CSCun00720	The UCS 6296 FI no longer fails to boot after a software upgrade, reload, or power cycle.	2.0(2m)A	2.2(3a)A
CSCun66874	DIMM blacklisting no longer prevents the host from accessing the DIMM bus.	2.2(2c)A	2.2(3a)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCun84951	MCA and MCE errors are now logged when a Cisco UCS blade server reboots due to a CPU CATERR fault.	2.2(1b)B	2.2(3a)B
CSCuo09991	The primary FI and secondary FI in a HA cluster no longer fail to sync after rebooting.	2.2(1b)A	2.2(3a)A
CSCuo34760	vEthernet interfaces and VIFs no longer remain in down state if the primary FI in a HA cluster is rebooted and comes up as the secondary FI.	2.1(2d)A	2.2(3a)A
CSCuo48978	Cisco UCS Manager now prevents downgrading the BIOS to an unsupported version on Cisco UCS C22, C24, C220, and C240 M3 servers with E5-2600 or E5-2400 v2 series CPUs.	2.1(2a)C	2.2(3a)C
CSCuo51708	Cisco UCS Manager downgrade no longer fails during autoinstall.	2.2(1d)A	2.2(3a)A
CSCuo76425	Ingress CRC errors are no longer seen over TwinA.x cables with rapid link-flaps on the 6248 and 6296 platforms	2.2(1c)A	2.2(3a)A
CSCuo80898	When upgrading an environment from Release 2.1(1a) to newer releases, the SAN port-channels that have member ports with different max speed will not be configured and a fault is raised to indicate this.	2.1(2a)A	2.2(3a)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCup05019	Status of FlexFlash controller no longer shows as 'Disconnected Partition From Host" and SD cards are now visible in the local disks option after inserting those cards into a blade with Flexflash enabled in local storage policy.	2.2(1d)A	2.2(3a)A
CSCup47504	Cisco UCS VIC 1240 adapter no longer fails to complete the PXE boot process due to missing DHCP offer on a Cisco UCS 6200 FI using an ASA as the DHCP relay.	2.2(1d)B	2.2(3a)B
CSCup61601	FI no longer crashes upon executing the show platform software fcoe_mgr info global command when there are too many noncontiguous VLANs configured.	2.2(1d)A	2.2(3a)A
CSCup61947	MAC learning no longer fails after adding 1,000 or more VLANs with a large PV count with 120 or more virtual interfaces each with 1,000 VLANs.	2.2(1d)A	2.2(3a)A
CSCup82677	Line rate is no longer limited to 10GB even when QoS line rate is set to 20GB or 40GB.	2.1(3b)A	2.2(3a)A
CSCup88087	Cisco UCS B200 M3 server with a single CPU no longer reports faults for a second CPU not present in the hardware.	2.1(3a)A	2.2(3a)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuo87059	After a chassis decommission and recommission, backplane ports on an IOM are no longer missing due to a NULL serial number being sent to the Cisco UCS Manager.	2.2(2c)B	2.2(3a)B

Resolved Caveats in Release 2.2 (2e)

The following caveats are resolved in Release 2.2 (2e)

Table 44: Resolved Caveats in Release 2.2 (2e)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCur01379	The security vulnerabilities identified by Common Vulnerability and Exposures (CVE) CVE-2014-7169, CVE-2014-6271, CVE-2014-6277, CVE-2014-7186, CVE-2014-7187, and CVE-2014-6278 are addressed.	2.0(1q)A	2.2(2e)A
CSCur16493	The UCSC-GPU-VGXK2 GPU adapter firmware has been updated to version 80.04.F5.00.03_2055.0552.01.08.	2.2(2a)B	2.2(2e)B

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCup45930	When upgrading the Cisco UCS B230 M2 server from Cisco UCS Manager Release 2.2(1x) to Cisco UCS Manager Release 2.2(2x) or from Cisco UCS Manager Release 2.2(2x) to Cisco UCS Manager Release 2.2(3x), or when upgrading the Cisco UCS C460 M4 server from Cisco UCS Manager Release 2.2(2x) to Cisco UCS Manager Release 2.2(3x), association no longer fails.	2.2(1e)A	2.2(2e)A

Resolved Caveats in Release 2.2 (2d)

The following caveats are resolved in Release 2.2 (2d)

Table 45: Resolved Caveats in Release 2.2 (2d)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCui12868	Some conditions that result in the chassis displaying a thermal sensor reading error due to third-party applications accessing the PCH SMBus or CPU SMBus controller have been fixed.	2.0(4b)B	2.2(2d)B
CSCun25692	M71KR-Q no longer runs out of heap and causes SAN boot failure while allocating memory to critical data structure.	2.2(1b)B	2.2(2d)B
CSCun79973	vNIC no longer hangs when QoS policy on a vNIC is changed while a Netflow session with transmit monitoring is active on that vNIC.	2.2(2c)A	2.2(2d)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuo34760	Veths/VIFs no longer remain in down state on a Primary FI that gets rebooted and comes back up as subordinate FI.	2.1(2d)A	2.2(2d)A
CSCuo79500	A vNIC with a usNIC connection policy no longer falsely shows as a Dynamic vNIC after a second vNIC with a usNIC policy is added.	2.2(1c)A	2.2(2d)A
CSCuo98011	Service dcosag no longer crashes during Infra firmware upgrade (ucs-k9-bundle-infra.2.2.2c.A.bin) if upgrade is initiated from Cisco UCS Central, when Cisco UCS Manager is registered to Cisco UCS Central using IPv4 address and image bundles are not present in Cisco UCS Manager.	2.2(2c)A	2.2(2d)A
CSCup07488	ECC sensors no longer read or report invalid “Upper Non-Recoverable” data when there are existing failed PECI transactions on a blade.	2.2(2c)B	2.2(2d)B
CSCup61601	FCOE_MGR no longer crashes when FI is configured with too many noncontiguous VLANs.	2.2(1d)A	2.2(2d)A
CSCup61947	MAC learning no longer fails after adding 1000 or more VLANs with a large PV count with 120 or more virtual interfaces each with 1000 VLANs.	2.2(1d)A	2.2(2d)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCup82677	A Cisco UCS system with ESXi OS is no longer limited to 10Gb speed when QoS is configured with line-rate of 20Gb or 40Gb.	2.2(1d)A	2.2(2d)A

Resolved Caveats in Release 2.2 (2c)

The following caveats are resolved in Release 2.2 (2c)

Table 46: Resolved Caveats in Release 2.2 (2c)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCtf73879	Cisco UCS Manager (GUI or CLI) no longer fails to report the local disk failures, faults, alarms, status, or disk errors/error codes from MegaRAID controller.	1.4(1)	2.2(2c)
CSCuh89441	RHEL6.3 SAN boot on M73KR-E no longer fails.	2.2(1b)	2.2(2c)
CSCuh92027	The cluster no longer gets stuck in switchover in progress mode when unplugging the primary FI's management port.	2.1(1a)A	2.2(2c)A
CSCuh99542	New SNMP user configured via Cisco UCS Manager now shows up in UCS NX-OS CLI.	2.1(1e)A	2.2(2c)A
CSCuj74570	B420 M3 with UCSB-MLOM-PT-01 installed no longer reboots for discovery when first IOM is upgraded to 2204XP.	2.1(2a)B	2.2(2c)B
CSCuj81245	OS kernel and adapter logs no longer report multiple FNIC aborts when user starts a heavy write operation to SAN disk.	2.2(1b)B	2.2(2c)B

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuj81385	GUI no longer returns PSUs have failed, please check input fault.	2.1(3a)B	2.2(2c)B
CSCuj84543	IOM no longer incorrectly reports that grid redundancy is lost while all PSUs are in Active PS state.	2.1(3a)A	2.2(2c)A
CSCul03508	Kernel memory no longer runs out and causes FI to reboot when running CA AIM tool with Cisco UCS Manager.	2.1(1d)A	2.2(2c)A
CSCul15865	Remote user logged in as admin with valid locales is now able to create, modify, and delete in other organizations apart from the locales downloaded so long as locales restriction is not applied to the admin profile.	2.2(1b)A	2.2(2c)A
CSCul44421	Error no longer encountered when accessing shared-storage during FI reboot, upgrade, or IOM reset.	2.1(2d)A	2.2(2c)A
CSCul74278	The server no longer fails to boot from the local disk in cases where the boot policy was initially configured only for SAN devices and is later modified to add local disk or local HDD device.	2.2(1b)A	2.2(2c)A
CSCul87625	FI no longer reports PSU failure when there is no real outage.	2.1(3a)A	2.2(2c)A
CSCul95341	Server no longer becomes unreachable after vNIC failover/failback.	2.2(1b)A	2.2(2c)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCum10869	IO throttle count option on the FC adapter policy is now 256 by default and range changed to ‘256 to 1024’ to remove confusion caused by default value of 16, which was interpreted by driver to mean 2048.	2.1(1f)A	2.2(2c)A
CSCum18805	Error message no longer received when pinging from peer FI's local-mgmt.	2.2(1b)	2.2(2c)A
CSCum19106	HDDs are displayed appropriately now in both Cisco UCS Manager and in BIOS for B200 M3.	2.2(1b)B	2.2(2c)B
CSCum19132	httpd_cimc.sh crash no longer seen when changing switch mode from End-Host to Switch mode and vice versa.	2.2(1b)A	2.2(2c)A
CSCum20965	Service profile now correctly disassociates from the blade when selecting “Disassociate Service Profile” from Cisco UCS Manager GUI.	2.2(1b)	2.2(2c)A
CSCum51302	User no longer receives 'switchport trunk allowed vlan none' configuration error on vEthernet configuration for VLAN change.	2.2(1b)A	2.2(2c)A
CSCum57954	Ping requests no longer timeout when configuring a B200 M3 with Cisco UCS VIC 1240 and Cisco UCS VIC 1280 with VM-FEX on the ESXi DVS while vMotioning a VM between two blades.	2.2(1b)	2.2(2c)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCum60793	Cisco UCS Manager no longer reports 'mount suspend success' to operations manager errors when UCS becomes unreachable or unregistered with Cisco UCS Central.	2.1(2c)	2.2(2c)A
CSCum63448	A Cisco UCS compute blade no longer requests a reboot for minor changes when a component firmware in an Activating state after an upgrade is completed.	2.1(2c)A	2.2(2c)A
CSCum82385	Allowed VLANs in vNIC now matches the allowed VLANs in vEthernet in NX-OS and vNICs no longer get updated when the service-profile is renamed.	2.1(3a)A	2.2(2c)A
CSCum84239	No longer have to be logged in as admin to be able to connect adapter.	2.2(1b)A	2.2(2c)A
CSCum84618	Installation of Win2008R2 no longer fails to reload after loading the disk.sys driver, preventing final installation steps to be completed.	2.1(3a)B	2.2(2c)B
CSCum87525	The httpd.sh process on the subordinate FI no longer crashes after upgrading to 2.2(2c) from 2.1(3a) via auto install.	2.2(1b)A	2.2(2c)A
CSCum95778	Incorrect sorting results are no longer displayed when attempting to sort a listing of service profiles and ORGs.	2.2(1b)A	2.2(2c)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCum98771	User no longer receives config failure message ‘Flexflash controller error, probably not supported, not equipped or inoperable’ when Cisco UCS Manager is updated from 2.1(2a) or above to 2.2(1) with FlexFlash State enabled.	2.2(1b)A	2.2(2c)A
CSCun13327	A Cisco UCS system with a high number of blade or rack-servers no longer experiences a high number of messages collected in the bladeAG logs, causing logs to overflow and prevent user from collecting necessary data for troubleshooting purposes.	2.1(3a)A	2.2(2c)A
CSCun14140	UCSB-B200-M3 Kernel no longer panics or hangs.	2.1(3b)B	2.2(2c)B
CSCun19372	User is no longer prevented from adding interface from both fabrics to the VLAN when launching the LAN Uplink Manager from the Equipment > Interconnects > Fabric Interconnect A (or B) path.	2.2(1b)A	2.2(2c)A
CSCun24381	Customers using the Cisco UCS PowerTool will no longer experience problems when scraping the Java log file for XML parsing of config changes when running Java version 7 update 45.	2.2(1b)A	2.2(2c)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCun25187	Cisco UCS Manager no longer becomes Lost-Visibility in Cisco UCS Central when keyring with certificate chain is configured for https communication if third-party certificates are signed by subordinate CA instead of root CA.	2.1(2a)A	2.2(2c)A
CSCun42280	Messages log no longer overfilled with BMC is suspecting that palo is in boot block. Leaving I2C bus alone. messages.	2.1(2a)B	2.2(2c)B
CSCun43320	Linux PXE server no longer fails to boot from gPXE server.	2.1(2a)B	2.2(2c)A
CSCun46196	A Cisco UCS running 2.2(2c) that has a M1 or M2 blade no longer reports a minor fault related to Inband configuration when there is actually no Inband configuration intended for that blade.	2.2(1b)	2.2(2c)A
CSCun94906	The Cisco UCS Manager DME no longer crashes when a SP is referring to a SP template and Cisco UCS Manager is connected to Cisco UCS Central during policy ownership conflict checks.	2.2(1b)B	2.2(2c)B

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCun95096	During association, the service profile no longer fails with an error stating that the RAID configuration is invalid due to an attempt to mix different drive technologies simply because one drive has an incorrect capability catalog technology field (set to HDD when it should be set to SSD).	2.2(1b)T	2.2(2c)T
CSCuo06886	Cisco UCS Manager no longer populates the Created at field with a strange number in the wrong format instead of the date when exporting events in CSV format.	2.2(1b)A	2.2(2c)A
CSCuo09527	A blade running on a 2-socket B420 M3 no longer boots to the BIOS screen after an update if the boot order is configured in the Cisco UCS Manager and the BIOS is set to strict mode.	2.2(1b)A	2.2(2c)A
CSCuo12965	KVM console no longer fails to launch when user tries to launch from the Equipment tab in Cisco UCS Manager or from the KVM Launch Manager due to erroneous ‘No management IP address set’ error message when server has no management IP addresses assigned but the associated service profile does.	2.2(1b)A	2.2(2c)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuo23630	User no longer receives “There are uncommitted changes” prompt after applying a port license to FI and, then, trying to move to another screen.	2.2(1c)A	2.2(2c)A
CSCuo30572	Intel v2 processors no longer cause PSOD with Microsoft Windows 2008 R2 VM guests.	2.1(3a)A	2.2(2c)A
CSCuo36008	User no longer receives the ‘peer connectivity: disconnected’ warning after re-seating the IOM(A).	2.2(1c)A	2.2(2c)A
CSCuo78883	Cisco UCS Manager and KVM users or admins using JRE version 1.7 update >= 40 no longer encounter a pop-up window with the 'Application Blocked by Security Settings' dialog.	2.0(1m)A	2.2(2c)A

Resolved Caveats in Release 2.2 (1h)

The following caveats are resolved in Release 2.2 (1h)

Table 47: Resolved Caveats in Release 2.2 (1h)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCut63966	Switch will not stop at loader prompt upon reboot due to incorrect boot variables or /opt corruption.	2.2(1b)A	2.2(1h)A, 2.2(3g)A
CSCur88952	svc_sam_dme core is no longer found after upgrading from or downgrading to Cisco UCS Manager Release 2.1(1b).	2.1(3g)A	2.2(1h)A, 2.2(3f)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCus83447	Cisco UCS Fabric Interconnect reload or switchover due to a leap second update no longer occurs.	2.2(1b)A	2.2(1h)A,2.2(3e)A
CSCus85186	After activating Cisco Trusted Platform Module (TPM), the enable and active statuses will not remain as disabled and deactivated.	2.2(1d)B	2.2(1h)B, 2.2(3j)B, 2.2(4b)B
CSCut03086	In a VM-FEX scale set up with over 100 servers, when you use auto install infrastructure firmware bundle and UCS Manager FI upgrades, DME core will not happen.	2.2(2c)A	2.2(1h)A, 2.2(3g)A
CSCur54705	Cisco UCS Manager will no longer send UCS Manager username and password hashes to the configured SYSLOG server every 12 hours.	2.1(1a)A	2.2(1h)A,2.2(3e)A
CSCut09151, CSCut21914 and CSCut08605	Traffic from the host and CIMC will no longer collide on the shared System Management BUS(SMBUS). As a result, certain system failures such as false thermal alarms will not happen.	2.1(3a)B	2.2(1h)A, 2.2(3f)B
CSCuo50049	Cisco UCS Manager will not experience HA cluster failover after upgrading from Release 1.4.	2.0(5g)A	2.2(1h)A, 2.2(3d)A

Resolved Caveats in Release 2.2 (1g)

The following caveats are resolved in Release 2.2 (1g)

Table 48: Resolved Caveats in Release 2.2 (1g)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuo51708	UCSM autoinstall downgrade no longer fails while reverting firmware during autoinstall process.	2.1(1f)A	2.2(1g)A
CSCuq70724	DIMM I2C controller is automatically reset if there are invalid I2C transactions that prevent the chassis from obtaining temperature readings from blades (which can cause fan speeds to spin at 100%).	2.1(1a)B	2.2(1g)B
CSCuq20755	Race conditions no longer occur due to DME crashing and restarting.	2.0(1q)A	2.2(1g)A
CSCuq74472	Unnecessary thermal events on IOM stating that the thermal sensor reading is not available no longer occur.	2.1(3c)A	2.2(1g)A
CSCur37260	FI upgrade or downgrade no longer fails due to lack of disk space in /mnt/pss.	2.1(3b)A	2.2(1g)A

Resolved Caveats in Release 2.2 (1f)

The following caveats are resolved in Release 2.2 (1f)

Table 49: Resolved Caveats in Release 2.2 (1f)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuq35685	IGMPv2 traffic no longer causes MAC flapping on upstream switches when the FI has multiple uplinks connecting to different switches.	2.2(1b)A	2.2(1f)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCur01379	The security vulnerabilities identified by Common Vulnerability and Exposures (CVE) CVE-2014-7169, CVE-2014-6271, CVE-2014-6277, CVE-2014-7186, CVE-2014-7187, and CVE-2014-6278 are addressed.	2.0(1q)A	2.2(1f)A
CSCuo34760	vEthernet interfaces and VIFs no longer remain in down state if the primary FI in a HA cluster is rebooted and comes up as the secondary FI.	2.1(2d)A	2.2(1f)A
CSCuq63086	Cisco B200 M3 no longer fails with a ‘Controller 1 on server x/y is inoperable’ error.	2.2(1e)B	2.2(1f)B

Resolved Caveats in Release 2.2 (1e)

The following caveats are resolved in Release 2.2 (1e)

Table 50: Resolved Caveats in Release 2.2 (1e)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCup61947	MAC learning no longer fails after adding 1000 or more VLANs with a large PV count with 120 or more virtual interfaces each with 1000 VLANs.	2.2(1d)A	2.2(1e)A, 2.2(2d)A
CSCul44421	Error no longer encountered when accessing shared-storage during FI reboot, upgrade, or IOM reset.	2.0(5f)B	2.2(1e)B

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCum98771	User no longer receives config failure message 'Flexflash controller error, probably not supported, not equipped or inoperable' when Cisco UCS Manager is updated from 2.1(2a) or above to 2.2(1) with FlexFlash State enabled.	2.2(1b)A	2.2(1e)A
CSCun24381	Customers using the Cisco UCS PowerTool will no longer experience problems when scraping the Java log file for XML parsing of config changes when running Java version 7 update 45.	2.2(1b)A	2.2(1e)A
CSCun25187	Cisco UCS Manager no longer becomes Lost-Visibility in Cisco UCS Central when keyring with certificate chain is configured for https communication if third-party certificates are signed by subordinate CA instead of root CA.	2.1(2a)A	2.2(1e)A
CSCun25692	M71KR-Q no longer runs out of heap and causes SAN boot failure while allocating memory to critical data structure.	2.2(1b)B	2.2(1e)B, 2.2(2d)B
CSCun83328	vNIC PCI addresses no longer get changed when downgrading from release 2.2(1e) to 2.0(5).	2.2(1d)B	2.2(1e)B
CSCun84897	Server reboots are no longer triggered when vNIC template is used with global service profile and customer changes MTU setting.	2.1(3a)A	2.2(1e)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuo78883	Cisco UCS Manager and KVM users or admins using JRE version 1.7 update >= 40 no longer encounter a pop-up window with the 'Application Blocked by Security Settings' dialog.	2.0(1m)A	2.2(1e)A
CSCuo79500	Cisco UCS Manager no longer falsely displays information that indicates a vNIC with a usNIC connection policy was automatically changed to dynamic vNIC when a customer adds a second vNIC with a usNIC policy.	2.2(1c)A	2.2(1e)A

Resolved Caveats in Release 2.2 (1d)

The following caveats are resolved in Release 2.2 (1d)

Table 51: Resolved Caveats in Release 2.2 (1d)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCui31011	VIFs and vNICs on the subordinate no longer fail to come up after FI failover.	2.1(2a)A	2.2(1d)A
CSCul38768	“Management services are unresponsive” fault no longer displayed in Cisco UCS Manager unless there is actually an HA condition failure.	2.1(1e)A	2.2(1d)A
CSCul96021	Frequent crashing of dcosAG process no longer occurs after Cisco UCS Manager upgrade.	2.2(1b)A	2.2(1d)A
CSCum02561	Server no longer reboots after infra-only upgrade that is followed by a service profile change.	2.2(1b)A	2.2(1d)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCum04646	FI no longer reboots while doing SNMP Walk with LDAP configuration enabled.	2.2(1b)A	2.2(1d)A
CSCum09954	Erroneous minor faults “FCoE” or “FC uplink is down” are no longer displayed in Cisco UCS Manager when FC uplink interfaces are admin shut.	2.2(1b)A	2.2(1d)A
CSCum75266	FIs no longer go to bash prompt during upgrade to 2.2 release.	2.2(1b)A	2.2(1d)A
CSCum82888	Access to Cisco UCS Manager, FIs, and Virtual IP is no longer blocked after upgrade or reboot if default keyring was deleted.	2.2(1b)A	2.2(1d)A
CSCun01514	Boot Order change via CLI or XML API no longer fails between SAN and other devices.	2.2(1b)A	2.2(1d)A
CSCun19289	The mgmt0 interface on an FI no longer drops traffic coming from blades behind that FI.	2.2(1b)B	2.2(1d)B
CSCun21077	Blades running ESXi OS will no longer hit a speed cap of 10GB when running on hardware that allows for higher speeds.	2.2(1b)A	2.2(1d)A
CSCun59192	Secure properties, such as authentication passwords and community strings, are no longer reset when importing a backup configuration that was created while being registered to Cisco UCS Central with admin policies managed globally.	2.2(1c)A	2.2(1d)A

Resolved Caveats in Release 2.2 (1c)

The following caveats are resolved in Release 2.2 (1c)

Table 52: Resolved Caveats in Release 2.2 (1c)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCum43435	The Cisco UCS VIC 1280 adapter on a Cisco UCS B440 M2 blade no longer hangs during PXE boot.	2.2(1b)B	2.2(1c)B
CSCul44120	Cisco UCS blade servers performing a PXE boot from a Citrix PVS system no longer fail after the initial bootloader initialization with a “No API found” error.	2.1(2a)B	2.2(1c)B
CSCum51025	Cisco UCS Manager domains registered in Cisco UCS Central no longer fail during scheduled backups.	2.2(1b)A	2.2(1c)A
CSCum25003	Associated local and global service profile inventory information is no longer sent to Cisco UCS Central when no changes are made.	2.2(1b)A	2.2(1c)A

Resolved Caveats in Release 2.2 (1b)

The following caveats are resolved in Release 2.2 (1b)

Table 53: Resolved Caveats in Release 2.2 (1b)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCug93342	After rebooting the FI during an upgrade, the FI no longer boots to the Loader prompt. **Note** To ensure the new power sequencer firmware is installed properly, you must power cycle the FI after the upgrade is completed.	2.1(3a)A	2.2(1b)A
CSCuc19701	The 2204 IOM no longer reboots when the FI is reset.	2.1(1a)A	2.2(1b)A
CSCuf90470	When Call Home is enabled, Online Insertion and Removal (OIR) or failure of hardware modules in the FI no longer causes the FI to reboot.	2.1(1b)A	2.2(1b)A
CSCui45963	Some of the text and controls are no longer truncated when you create a service profile or service profile template using the wizard.The edit option for storage settings is enabled.	2.1(2a)A	2.2(1b)A
CSCuj84421	Installing Java 7 update 45 no longer causes UCS Manager GUI failures.	2.1(1f)A	2.2(1b)A
CSCuc38783	Firmware upgrade no longer fails on BRCM 57712 adapter.	2.1(1a)A	2.2(1b)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuj77813	Associating service profile to a C-series server integrated with Cisco UCS Manager no longer fails.	2.1(3a)C	2.2(1b)A
CSCui43905	When you try to create an iSCSI NIC on a service profile, UCS Manager no longer displays any warning messages.	2.1(2a)B	2.2(1b)A
CSCuj32124	During normal operation IOM no longer unexpectedly reboots with CPU reset.	1.4(2b)A	2.2(1b)A
CSCui41165	Cisco UCS Manager no longer displays “error accessing shared-storage”error or have the following issues: • Call home fan alerts are sent and cleared immediately • Errors during IOM boot-up	1.4(2b)A	2.2(1b)A
CSCuj78099	FC traffic between a Cisco UCS FI and a Cisco MDS switch is no longer disrupted when the FI is in switch mode.	2.1(3a)A	2.2(1b)A
CSCuj61839	With the 2.2(1b)B bundle, Cisco UCS Blade servers on a Cisco M81KR VIC adapter no longer encounter ASSERT FAILED @ mips/ecpu_pani.c:138 errors.	2.1(2a)A	2.2(1b)A
CSCuj10564	Discard TX on a FC trunk port are no longer seen after hot-swapping the Cisco UCS-FI-E16UP expansion module on the Cisco UCS 6248UP FI.	2.1(1f)A	2.2(1b)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuf77316	Windows 2012 installed on a FlexFlash card no longer fails Microsoft certification.	2.1(2a)B	2.2(1b)A
CSCui87195	The FLS process on Cisco CNA M72KR-E no longer cores with the following message: `130820-19:06:33.645547 fls.fc vnic 15: Local port down for lif 4.`	2.0(5c)C	2.2(1b)A
CSCuj99958	During heavy FC traffic, the server no longer stops responding with an `ASSERT FAILED (Exception 2 triggered!) @ mips/ecpu_panic.c:138` error.	2.1(1f)A	2.2(1b)A
CSCug89448	The tech support collection no longer fails on the Cisco UCS Manager GUI.	2.0(1s)A	2.2(1b)A
CSCug63368	PXE boot no longer fails in vPC environments if the DHCP relay agent is installed as the gateway IP address during a PXE boot instead of the HSRP IP address.	2.1(1d)B	2.2(1b)A
CSCui82679	FlexFlash storage is no longer disconnected from a Cisco B200 M3 server after booting ESX or ESXi from a FlexFlash card.	2.1(2a)A	2.2(1b)A
CSCuc52981	Downloaded license files for FIs continue to be displayed in the downloads area after installation.	2.0(3a)A	2.2(1b)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCti39470	RAID 50 and RAID 60 configurations can now be created and managed by Cisco UCS Manager.	1.4(1i)A	2.2(1b)A

Open Caveats

The open bugs for a release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains up-to-date information about bugs and vulnerabilities in this product and other Cisco hardware and software products.

Note You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. If you do not have one, you can register for an account.

For more information about the Cisco Bug Search Tool, see the Bug Search Tool Help & FAQ.

Open Caveats in Release 2.2(8g)

The following caveats are open in Release 2.2(8g)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvb48577	UCS Manager includes a version of OpenSSL that is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) IDs: 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	There is no known workaround.	2.2(8g)B Resolved in 2.2(8i)B

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvb61637	A vulnerability in the CLI of the Cisco Unified Computing System Manager could allow an authenticated, local attacker to perform a command injection attack. The vulnerability is due to insufficient input validation for the affected command. An authenticated local attacker could exploit this vulnerability by injecting crafted command arguments into a redirect of a vulnerable CLI command. An exploit could allow the attacker to execute arbitrary system commands with the privileges of the authenticated user. UCS Manager is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) IDs: CVE-2017-6600	There is no known workaround.	2.2(8g)A Resolved in 2.2(8i)A
CSCvb86764	A vulnerability in the CLI of the Cisco UCS Manager could allow an authenticated, local attacker to perform a command injection attack. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by injecting crafted command arguments into a vulnerable CLI command. An exploit could allow the attacker to read or write arbitrary files at the user's privilege level outside of the user's path. UCS Manager is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) IDs: CVE-2017-6601	There is no known workaround.	2.2(8g)A Resolved in 2.2(8i)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvb86775	A vulnerability in CLI of the Cisco Unified Computing System Manager could allow an authenticated, local attacker to perform a command injection attack. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by injecting crafted command arguments into a vulnerable CLI command. An exploit could allow the attacker to read or write arbitrary files at the user?s privilege level outside the expected path and gain access to other devices. The vulnerability is identified by the following Common Vulnerability and Exposures (CVE) IDs: CVE ID CVE-2017-6602	There is no known workaround.	2.2(8g)A Resolved in 2.2(8i)A
CSCvb86797	A vulnerability in the debug plugin functionality of the Cisco Unified Computing System Manager could allow an authenticated, local attacker to execute arbitrary commands. The vulnerability is due to inadequate integrity checks for the debug plugin. An attacker could exploit this vulnerability by crafting a debug plugin and load it using elevated privileges. An exploit could allow the attacker to run malicious code that would allow for the execution of arbitrary commands as root. The vulnerability is identified by the following Common Vulnerability and Exposures (CVE) IDs: CVE ID CVE-2017-6598	There is no known workaround.	2.2(8g)A Resolved in 2.2(8i)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvb86816	A vulnerability in local-mgmt CLI of the Cisco Unified Computing System Manager could allow an authenticated, local attacker to perform a command injection attack. The vulnerability is due to insufficient input validation for the affected command. An authenticated local attacker could exploit this vulnerability by injecting crafted command arguments into a vulnerable CLI command. An exploit could allow the attacker to execute arbitrary system commands with the privileges of the authenticated user. The vulnerability is identified by the following Common Vulnerability and Exposures (CVE) IDs: CVE ID CVE-2017-6597	There is no known workaround.	2.2(8g)A Resolved in 2.2(8i)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvc37931	Unvalidated redirects and forwards may be possible when UCS Manager accepts untrusted input that could cause it to redirect the request to a URL contained within untrusted input. By modifying untrusted URL input to a malicious site, an attacker may successfully launch a phishing scam and steal user credentials. Unvalidated redirect and forward attacks can also be used to maliciously craft a URL that would pass the application�s access control check and then forward the attacker to privileged functions that they would normally not be able to access. The vulnerability is identified by the following Common Vulnerability and Exposures (CVE) IDs: CVE ID CVE-2017-6604 Impacted Unified Computing System (UCS) B-Series M3 and M4 Blade Servers Affects any of the 2.2(8) and 3.1(2) blade bundle versions. None of the 3.0 or 3.1(1) blade bundle versions. Impacted Unified Computing System (UCS) C-Series M3 and M4 Rack Servers Affects 3.0(1c) CIMC versions. None of the 1.5 or 2.0 CIMC versions.	There is no known workaround.	2.2(8g)A Resolved in 2.2(8i)A
CSCvc58789	A port may get a disabled error from 10 consecutive DFE tuning failures.	If this is encountered, try the following steps: • Unplug and re-insert cable or SFP • Try replacing the cable or SFP. • Disable and then re-enable the link from UCSM (equivalent of shut / no shut from NxOS).	2.2(8g)A Resolved in 2.2(8i)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvc94686	UCS Manager includes a version of OpenSSL that is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) IDs: CVE-2017-3731 - Truncated packet could crash via OOB read. This product is not affected by the following vulnerabilities: CVE-2017-3730 - DHE parameters cause a client crash CVE-2017-3732 - BN_mod_exp may produce incorrect results on x86_64	There is no known workaround.	2.2(8g)A Resolved in 2.2(8i)A
CSCvc96103	UCS Manager includes a version of OpenSSL that is affected by the vulnerability identified by one or more of the following Common Vulnerability and Exposures (CVE) IDs: CVE-2017-3731 CVE-2017-3730 CVE-2017-3732 And disclosed in [illegible]	There is no known workaround.	2.2(8g)A Resolved in 2.2(8i)A
CSCve19522	UCS Domains running version 3.1(3a) may move to a state of lost visibility after a certificate is regenerated on UCS Central and could fail to recover. In some cases, the UCS 3.1(3a) domain registration may also get stuck in a registering state.	Use one of the following workarounds to recover the system: • Upgrade to UCSM 3.1(3b). • Load debug plugin in UCSM and restart the httpd process manually. • UCSM# ps -aef|grep -i httpd.sh ==>To get the process id for httpd.sh • UCSM# kill -9 <httpd.sh process_id> • Perform a pmon restart on both nodes of UCSM, which will intern restart the httpd along with other processes.	2.2(8g)A Resolved in 2.2(8i)A

Open Caveats in Release 2.2(8d)

Open Caveats in Release 2.2(8d)

Table 54: Open Caveats in Release 2.2(8d)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvb11667	Server with UEFI BIOS enabled, may fails to SAN boot from a target LUN with an ID other than 0 and using T10 DIF protection.	When this issue occurs, set the BIOS to legacy mode or use LUN ID 0.	2.2(8d)B Resolved in 2.2(8f)B
CSCvb82862	EUI-64 bit addresses were invalid for storage connection policies or SAN boot targets.	There is no known workaround.	2.2(8d)A Resolved in 2.2(8f)A
CSCvb95978	On C460 M4 servers, TPM version 1.2 may fail to initialize after installing ESXi OS, and enabling and activating TPM and TXT.	There is no known workaround.	2.2(8d)B Resolved in 2.2(8f)B

Open Caveats in Release 2.2(8c)

Open Caveats in Release 2.2(8c)

Table 55: Open Caveats in Release 2.2(8c)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvd54116	Setting a custom cipher suite for UCS Manager HTTPS to remove the usage of TLS v1.0 and 1.1, may result in a ""handshake failure"" error message when attempting to open a Java login to UCS Manager or a KVM session to a blade server.	Explicitly allow AES128-SHA in the custom cipher to allow logins to UCS Manager. This does not affect UCS Manager versions that have the HTML5 login higher than 3.1, as the custom suite is adhered to. However, if a KVM session is opened then the failure will be seen as well, as this is still uses Java.	2.2(8c)A Resolved in 2.2(8i)A

Defect ID	Symptom	Workaround	First Bundle Affected

CSCvb85331	The following fault may occur after a UCS Manager software upgrade.
	Code: F1781
	Description: Management database version mismatch detected failover may not complete
	Affected Object: sys/mgmt-entity-B
	Name: Mgmt Entity Mgmt Db Version Mismatch
	Cause: Replication Failure
	Type: Management
		Restart the process monitor on the subordinate FI with the following commands:
		`connect local-mgmt (A/B)`
		`pmon stop`
		`pmon start`
		`show pmon state`
			2.2(8c)A
			Resolved in 2.2(8g)A

CSCvb47285	In the process of rebooting the fabric interconnect and collection of tech support logs, a core file was generated.	There is no known workaround.	2.2(8c)

Open Caveats in Release 2.2(8b)

Open Caveats in Release 2.2(8b)

Table 56: Open Caveats in Release 2.2(8b)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvb00303	During a Server discovery, Rack servers may get stuck and may not discover due to a lost connection status from B side while only A side is appearing. This may occur after upgrading to 2.2(8b) and performing an Erase Samdb operation and then enabling all required server ports to bring the server up.	There is no known workaround.	2.2(8b)A Resolved in 2.2(8h)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvc60876	The 6248, 6296, and 6332 Series Fabric Interconnects may send Smart Call Home messages in the wrong format.	Contact the Smart Call Home support team to fix the XML file and reprocess the message.	2.2(8b)A Resolved in 2.2(8g)A
CSCva96740	Changes in adapter policy from UCS Manager did not trigger a server redeploy.	Manually schedule a reboot for the Service Profile for the FC Adaptor policies to be reflected.	2.2(8b)A Resolved in 2.2(8c)A

Open Caveats in Release 2.2(8a)

Open Caveats in Release 2.2(8a)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvf32853	Blade upgrades may fail to boot and get stuck at "Waiting for BIOS POST completion" during a firmware update for storage controllers.		3.1(3a)B 2.2(8a)B

Defect ID	Symptom	Workaround	First Bundle Affected
		Create two host firmware packages: Create a Host Firmware Package for your target version that Excludes "Storage Adapters". This is only possible in UCSM 2.2(7b) and later. In previous versions you will have to create an Advanced Host Firmware Package and select all components except the Storage Adapters. Create a second Host Firmware Package that ONLY includes the Storage Adapters and select the versions that you are looking to upgrade to. You can do this by Excluding all other components, or by making an Advanced Host Firmware Package. How to upgrade the servers: To upgrade the servers, first upgrade all the components EXCEPT the Storage Adapter. So we will use the first Host Firmware Package created. Update the RAID Controller by itself by selecting the second Host Firmware Package created. You can now assign the Service Profile back to the original Host Firmware Package. Since all components have been upgraded, no further changes will be made.	

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuz52483	UCS Manager includes a version of OpenSSL that may be affected by the vulnerabilities identified by the Common Vulnerability and Exposures (CVE) IDs: CVE-2016-2108 CVE-2016-2107 CVE-2016-2105 CVE-2016-2106 CVE-2016-2109 CVE-2016-2176	There is no known workaround.	2.2(8a)A Resolved in 2.2(8i)A
CSCvc31867	When upgrading the SSD to firmware 32F3Q, the firmware may be truncated and written as 2F3Q, which may cause a second request for the reboot of the server.	Exclude the Local Disk Firmware update from the Host Firmware Package (HFP) in the associated Service Profile.	2.2(8a)A Resolved in 2.2(8g)A
CSCuy81688	From Cisco UCS Manager tech-support, running /var/sysmgr/sam_logs/httpd_cimc.log on the affected fabric interconnect may show the exceeded max time without restart error. From Cisco UCS Manager tech-support, running /ls_l.out on the affected fabric interconnect may show the existence of a 'cimcrestart' file under /isan/apache/conf/. The modified date is now updated.	If this issue occurs, do the following: • Using the debug plugin, delete the file /isan/apache/conf/cimcrestart. • Stop and start the UCSM processes using 'pmon stop'/'pmon start'.	2.2(8a)A Resolved in 2.2(8f)A
CSCvb16804	Booting from SAN to 4K UEFI target may fail.	There is no known workaround.	2.2(8a)B Resolved in 2.2(8f)B
CSCuy65407	The VIC adapter may go into an inaccessible state while flapping RNICs that run high block size read/write workloads.	When this issue occurs, power cycle the server to reboot the VIC.	2.2(8a)B, 2.2(8a)C

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuz41121	When booting to RHEL or running system stress tests, Cisco UCS B420 M4 servers with certain Intel ® E5 v3 CPUs may report QPI Correctable System Event Logs with the following error message: `Link Layer CRC successful reset with no degradation` These System Event Logs are benign and do not impact system operation.	There is no known workaround.	2.2(8a)B Resolved in 2.2(8c)B
CSCuz76717	The ESX host reboot hangs while loading the ENIC module with NetFlow enabled.	If this issue occurs, do the following: • Disable Netflow • Reboot the system • Enable NetFlow	2.2(8a)B, 2.2(8a)C
CSCuz79138	The host becomes unresponsive when using second generation VIC adapters while running FCOE traffic and Ethernet traffic on the same side of the fabric with NetFlow enabled.	No known workaround for second generation VIC adapters. You can enable NetFlow with third generation VIC adapters or later generation adapters.	2.2(8a)B, 2.2(8a)C
CSCva36835	When using Cisco B460 M4 or B260 M4 blade servers, a warm boot does not reset the LSI controller.	There is no known workaround.	2.2(8a)B Resolved in 2.2(8b)B

Defect ID	Symptom	Workaround	First Bundle Affected
CSCva38325	C460 M4 systems under heavy CPU/memory load can report Machine Check Exceptions in Linux syslog and/or correctable QPI errors in the System Event Log. These MCE and SEL are benign and do not impact system operation.	There is no known workaround.	2.2(8a)C

Defect ID	Symptom	Workaround	First Bundle Affected

CSCva67159	Cisco UCS Manager httpd failed to start when the default keyring was deleted.	If this issue occurs, do the following:
		• Create default certificate.
		• Disable and Enable http and https service from CLI If http-redirect is disabled, then disable and enable http-redirect service. At this stage, user will be able to access UCSM GUI
		• UCSM GUI will be still referencing default self-signed certificate. Please contact TAC to configure HTTPD to use customer (third party) certificate
		`UCS # scope security`
		`UCS /security # create keyring default`
		`UCS /security/keyring* # set modulus mod2048`
		`UCS /security/keyring* # commit-buffer`
		`UCS /security/keyring # top`
		`UCS # scope system`
		`UCS /system # scope services`
		`UCS /system/services # disable https`
		`UCS /system/services* # disable http`
		`UCS /system/services* # commit-buffer`
		`UCS /system/services # enable http`
		`UCS /system/services* # enable https`
		`UCS /system/services* # commit-buffer`
			2.2(8a)A
			Resolved in 2.2(8b)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCva71801	UCS Manager may fail to synchronize with an IPv6 NTP server.	If possible, drop into the debug plugin and restart the ntpd process by using the command: `killall ntpd` Or change the IPv6 NTP server to a IPv4 NTP server.	2.2(8a)A Resolved in 2.2(8c)A
CSCva87230	Temporary loss in server connectivity may be experienced when performing a Cisco UCS Manager upgrade to release 2.2(8a) from a build that does not contain the fix for CSCuq57142.	Upgrade Cisco UCS Manager software to a release that has the fix for CSCuq57142 before upgrading to release 2.2(8a). See the Software Advisory. **Note** CSCuq57142 has been fixed for 3.0(2c), 2.2(7c), 2.2(6c), and 2.2(3k).	2.2(8a)A Resolved in 2.2(8b
CSCvb35827	Upgrade failure occurs when the Cisco UCS system is configured with more than 128 LDAP groups and upgrade is performed either from Cisco UCS Manager Release 2.2.8 to Cisco UCS Manager Release 3.1(2b) or from Cisco UCS Manager Release 3.1(2b) to a later release. The following error message is displayed: `Error: Update failed: [System has more than 128 LDAP groups set, Downgrade will cause ldapd crash, Delete the additional groups]`	If this issue occurs, do the following: • Create a backup of the configuration and reduce the number of LDAP groups to a value below or equal to 128. • After upgrade, re-apply the configuration.	2.2(8a)A Resolved in 2.2(8c)A

Open Caveats in Release 2.2(7c)T

Open Caveats in Release 2.2(7c)T

Table 57: Open Caveats in Release 2.2(7c)T

Defect ID	Symptom	Workaround	First Bundle Affected
CSCva53726	UCS Manager allows downgrade of firmware for the following rack servers installed with v4 CPU models to a version less than the minimum required version of CIMC / BIOS firmware: • UCSC-C240-M4L • UCSC-C240-M4S • UCSC-C240-M4S • UCSC-C240-M4SX • UCSC-C220-M4L • UCSC-C220-M4S • UCSC-C240-M4SNEBS After a downgrade, servers may fail during the BIOS post.	If the service profile is using the host firmware package policy with an older version, remove the older version from the policy. If UCS Manager is configured with auto-sync firmware policy, remove the older version from the auto-sync policy. After making the above changes, upgrade and activate the CIMC and BIOS to a minimum required version or via host firmware policy. Minimum CIMC / BIOS version required for v4 CPU model can be found in the following documents: • Cisco UCS B200 M4 Server Upgrade Guide for E5-2600 v4 Series CPUs • Cisco UCS C-Series Servers Upgrade Guide for Intel Xeon v4 Series CPUs	2.2(7c)T Resolved in 2.2(8d)T

Open Caveats in Release 2.2(7c)

Open Caveats in Release 2.2(7c)

Table 58: Open Caveats in Release 2.2(7c)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvc17769	The fabric interconnect may crash when the bound interface of a Veth is in the Not Initialized State during a VLAN configuration change.	If the bound interface of Veth is not initialized, then do not perform a VLAN configuration change on the Veth.	2.2(7c)A Resolved in 2.2(8f)A
CSCva34426	Cisco UCS 3X60 Server failed to boot from the LSI RAID controller managed disk slots 1 or 2, when the disks were in JBOD mode.	If this issue occurs remove the internal riser based SSDs and reacknowledge the server.	2.2(7c)A Resolved in 2.2(8b)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCva53726	UCS Manager allows downgrade of firmware for the following rack servers installed with v4 CPU models to a version less than the minimum required version of CIMC / BIOS firmware: • UCSC-C240-M4L • UCSC-C240-M4S • UCSC-C240-M4S • UCSC-C240-M4SX • UCSC-C220-M4L • UCSC-C220-M4S • UCSC-C240-M4SNEBS After a downgrade, servers may fail during the BIOS post.	If the service profile is using the host firmware package policy with an older version, remove the older version from the policy. If UCS Manager is configured with auto-sync firmware policy, remove the older version from the auto-sync policy. After making above changes, upgrade and activate the CIMC and BIOS to minimum required version or via host firmware policy. Minimum CIMC / BIOS version required for v4 CPU model can be found in the following documents: • Cisco UCS B200 M4 Server Upgrade Guide for E5-2600 v4 Series CPUs • Cisco UCS C-Series Servers Upgrade Guide for Intel Xeon v4 Series CPUs	2.2(7c)T Resolved in 2.2(8d)T

Defect ID	Symptom	Workaround	First Bundle Affected
CSCux11611	Seagate hard drives left spinning idle without an operating system installed or setup with the JBOD configuration without read or write activity were prone to failure. Impacted hard drives are listed here: • UCS-HD4T7KS3-E • UCSC-C3X60-HD4TB (4TB) • UCS-HDD3TI2F214 (3TB) • UCS-HDD2TI2F213 (2TB) • UCS-HDD1TI2F212 (1TB) • UCS-HD6T7KL4K • UCSC-C3X60-HD6TB • UCSC-C3X60-6TBRR	Do not leave idle systems powered on for extended periods of time. Either install an OS with all drives formatted or configure drives in a RAID configuration other than JBOD or JBOD equivalent and fully initialize the Virtual Drive(s).	2.2(7c)B Resolved in 2.2(8c)B
CSCux53224	A fatal error may be observed when you create or remove virtual drives with RAID 5 and RAID 6 controller combination.	No known workaround.	2.2(7c)C Resolved in 2.2(7d)C

Open Caveats in Release 2.2(7b)

Open Caveats in Release 2.2(7b)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuz98957	UCS Manager may incorrectly report the amount of drive slots on B200-M2 blade servers.	There is no known workaround.	2.2(7b)A Resolved in 2.2(8i)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvc39322	For B260 M4 Blades, BIOS v3.1.2.2 may intermittently fail Windows HLK and HCK Trusted Platform Module (TPM) tests on Windows Server 2016 and Windows Server 2012 R2.	Toggle the BIOS "TXT Support" setting to disable.	2.2(7b)B Resolved in 2.2(8g)B
CSCva35757	Latency between the UCS Manager Client and fabric interconnect may cause the firmware page to load slowly.	Use the CLI to complete upgrade or downgrade procedures.	2.2(7b)A Resolved in 2.2(8f)A
CSCvb05762	UCS Manager GUI and CLI may fail to respond when the Data Management Engine (DME) hangs with a WaitOnLimit log message.	Restarting the process monitor on the primary node resolves the issue.	2.2(7b)A Resolved in 2.2(8d)A
CSCva08256	Cisco CIMC and BIOS no longer get stuck updating or activating with the host firmware pack when the new host firmware pack has the same name and version as the system being updated.	Create a host firmware pack with a different name than the one already in the organization or the sub-organization levels.	2.2(7b)A Resolved in 2.2(8b)A
CSCva38476	An infrastructure software upgrade to UCS Manager 2.2(7b) or higher can fail when both fabric interconnects are incompatible or when one of the fabric interconnects are unresponsive.	Contact TAC to apply a workaround.	2.2(7b)A Resolved in 2.2(8c)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuy93451	When you create a vNIC from an updating vNIC template, and then delete vLANs from the updating vNIC template, these VLANs are not deleted from the vNIC.	When this issue occurs, do the following: • Unbind the vNIC from the vNIC template on the service profile or service profile template. • Delete the VLANs from the vNIC. • Bind the vNIC back to the vNIC template.	2.2(7b)A Resolved in 2.2(7c)A
CSCuz54661	Cisco B200 M3 Server failed to post if NUMA is disabled.	Enable NUMA optimization in the BIOS policy. Then perform a reset CMOS from the Recover Server options. This reboots the server and must be done to recover and stop the errors. **Note** If NUMA must stay disabled, the only workaround is to use 2.2(6d) or lower that doesn't contain BIOS version B200M3.2.2.6c.0.110420151250.	2.2(6g)B Resolved in 2.2(8b)B
CSCuz08759	The vniccfgd process no longer crashes when upgrading the VIC firmware contained in the server bundle to version 2.2(7b)B or 2.2(7b)C.	When this issue occurs, revert back to the previous firmware version before the downgrade occurred.	2.2(7b)B 2.2(7b)C Resolved in 2.2(7c)B 2.2(7c)C
CSCuz69373	During Cisco UCS Manager upgrade to release 3.1(1), you will see CATERR faults due to unresponsive eCPUs. This issue happens when the eCPUs fall into diagnostic code (debug loop) after the DINT CPU input is asserted.	No known workaround.	2.2(7b)B Resolved in 2.2(7c)B

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuy74364	When the CIMC version in the server is earlier than the 2.2(7) C Series bundle CIMC version, or, when the BIOS version in the server is later than the 2.2(6) C Series BIOS version, the host reboot is triggered along with a BIOS upgrade even for any unrelated service profile modification.	To avoid this issue, ensure that the server has BIOS and CIMC versions from the same C Series bundle.	2.2(7b)C
CSCva29365	Enabling stateless offloads for NVGRE in a 3rd generation Cisco VIC adapters' configuration with UCSM/CIMC leads to inaccessible vNIC interfaces in the host OS for the following 3rd generation VIC adapters: • UCSC-C3260-SIOC • UCSB-VIC-M83-8P • UCSB-MLOM-40G-02 • UCSB-MLOM-40G-03 • UCSC-PCIE-C40Q-03 • UCSC-MLOM-C40Q-03 This affects only the managed UCS deployments and standalone NIV mode deployments. Classical Ethernet operation is unaffected.	Disable stateless offloads for NVGRE in a 3rd generation Cisco VIC adapters.	2.2(7b)B Resolved in 2.2(7d)B

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuz69100	Disk Firmware update fails on a C240 rack server with a UCSC-SAS12GHBA storage controller in one of the following scenarios: • when more than ten disks are discovered • when certain Seagate HDD models are used This issue occurs if Cisco UCS Manager fails to map the local disk to its native SCSI device name because of a mismatched serial number between them.	No known workaround.	2.2(7b)A Resolved in 2.2(7d)A
CSCuz65286	Cisco UCS Manager firmware upgrade fails with the following message UCSM upgrade validation failed if the default value for IO throttle count in the FC adapter policy has a value of 16.	Before starting the upgrade, change the following: • Change the maintenance policy to user-ack. • Change the IO throttle count value to 256.	2.2(3a)A Resolved in 2.2(7d)A

Open Caveats in Release 2.2(6f)

Open Caveats in Release 2.2(6f)

Table 59: Open Caveats in Release 2.2(6f)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCux21413	When you remove and reinsert a drive in the same slot, the Locator Storage Locator LED may remain on all the time.	There is no known workaround.	2.2(6f)B Resolved in 2.2(7b)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCux07578	Cisco UCS Blade servers B400 M1 or B400 M2 running on firmware version 4.10 with SATA drives, may experience data consistency failures.	There is no known workaround.	2.2(6f)B Resolved in 2.2(7b)A
CSCuw46478	The Local disk Locator LED remains OFF, although enabled in Cisco UCS Manager.	There is no known workaround.	2.2(6f)B Resolved in 2.2(7b)B
CSCuv45574	On C220/C240 M3 systems with LSI 9271-8i controller, after downgrading the firmware to Release 2.0(3f) or lower with HUU update all, the virtual machines running on the ESXi OS become inaccessible. SUSE operating systems are also impacted and will not boot after upgrade.	See the following VMware knowledge base: http://kb.vmware.com/kb/1011387 (vSphere handling of LUNs detected as snapshot LUNs (1011387))	2.2(6f)A Resolved in 2.2(7d)A

Open Caveats in Release 2.2(6d)

The following caveats are open in Release 2.2(6d)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCux49157	UCS Manager now has a user configurable option to select the TLS version.	This is an enhancement request for a feature to explicitly allow the selection of the TLS Version. Custom Cipher Suites can be used to force the Client side to use a higher version.	2.2(6d)A Resolved in 2.2(8i)A

Open Caveats in Release 2.2(6e)

Open Caveats in Release 2.2(6e)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvc92275	A kernel panic may occur on the Fabric Interconnect and could cause a reboot. The command: `show logging onboard stack-trace` shows that the panic may occur in the process usd_mts_kthread. The call trace can be reviewed for a full match to this defect.	Apply rate limiting or other QOS policies upstream to prevent large amounts of traffic from hitting the mgmt interfaces of the fabric interconnects. Apply ACL on upstream devices to only allow connectivity to mgmt interfaces from approved or identified bastion hosts.	2.2(6e)A Resolved in 2.2(8i)A
CSCux96072	During heavy I/O traffic, the Cisco 12G Modular RAID controller may go offline with the Storage Controller SLOT HBA inoperable error logged in the CIMC event logs.	A fix is available in UCS Manager 2.0.10e and 2.0.13. Upgrade the Storage controller firmware and its corresponding driver.	2.2(6e)C Resolved in 2.2(8g)C

CSCvc89242	The Fabric Interconnect may reboot due to a CDP process crash.	If CDP still crashes immediately after the fabric interconnect reboot, execute the following commands to avoid another FI reboot.
		`connect nxos`
		`system no hap-reset`
		Contact TAC with the CDP core dump files if the reboot occurs again.
			2.2(6e)A
			Resolved in 2.2(8g)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuv43349	During server discovery, Cisco UCS Blade server association or disassociation, the following failures may be reported: • `Waiting for BIOS Post Completion` • `Unable to get SCSI Device Information from the system`	When this issue occurs, do the following: 1. Remove all of the Local Disks from the failed blade server. 2. Reboot the server without any Local Disks.	2.2(6e)B Resolved in 2.2(7b)B
CSCuz96855	UCS M71KR cards could crash with the error "E4194871".	Reduce the number of targets zoned with the initiator.	2.2(6e)A Resolved in 2.2(8c)B
CSCva34343	The P0V75_STBY sensor may throw an alert incorrectly on Cisco B200M4 servers.	There is no known workaround.	2.2(6e)B Resolved in 2.2(8c)B
CSCux47667	Service profile association to a server fails if the service profile was previously associated to a different server, and a LUN was deployed.	Delete the LUN configuration of the service profile before associating to a different server.	2.2(6e)A Resolved in 2.2(6f)A
CSCva01733	PXE in Legacy Boot mode fails if there is an excessive unicast or multicast high background traffic with a packet size larger than MTU directed to the client server. This was seen with ESXi Autodeploy on a specific setup which likely had unusually high multicast traffic directed at the client server. This traffic was not from the PXE server for file transfer, but from some other source.	Reduce excessive unicast or multicast background traffic directed to the client server.	2.2(6e)B Resolved in 2.2(6j)B 2.2(7d)B

Open Caveats in Release 2.2(6c)

Open Caveats in Release 2.2(6c)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvg06830	After adding a secondary fabric interconnect to a standalone setup and converting it to clustered setup, the VLAN 1 may not be added to the uplink port-channel, and could cause vEth on the B side to fail pinning and render the subordinate FI unusable.	If vNIC uplink pinning is not occurring on the subordinate fabric interconnect, consider removing the VLAN (in this case VLAN 1) configuration from the vNIC to allow uplink pinning and high availability.	2.2(6c)A Resolved in 2.2(8i)A
CSCvc88543	Cisco UCS Manager includes a version of the Apache HTTP Server software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs: CVE-2016-0736, CVE-2016-2161, CVE-2016-5387,CVE-2016-8740, CVE-2016-8743	There is no known workaround.	2.2(6c)A Resolved in 2.2(8i)A
CSCuw19082	During Cisco UCS Manager initial setup, while configuring the fabric interconnect, setup will assume the GUI configuration method if a DHCP lease is obtained for the mgmt interface. In addition, an url will be provided for the setup of the fabric interconnect.	There is no known workaround.	2.2(6c)A Resolved in 2.2(7b)A
CSCux66675	Rebooting a Cisco UCS 6296UP FI causes all physical interfaces to connect incorrectly with the Cisco UCS C460 M4 servers.	Reacknowledge the servers to resolve this issue.	2.2(6c)A Resolved in 2.2(7b)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCux98751	Anytime a new blade is inserted into the chassis, or a blade CIMC controller reboots, a chassis thermal fault may get generated because of the long time taken to reconnect from the IOM to the CIMC. This issue is caused by added time for BIOS Power Capping and SMBUS protection abilities.	This fault will clear by itself, and has no known workaround.	2.2(6c)B Resolved in 2.2(6g)B
CSCuw44524	Server reboot with 'Uncorrectable error ECC errors' may occur when you initiate a 'clear CMOS' operation in Cisco UCS Manager Release 2.2(5a), 2.2(5b), 2.2(5c) or 2.2(6c) for E7 v2 processors on the C460 M4, B260 M4, and B460 M4 servers.	Use the HUU or IMC interfaces to upgrade the BIOS again to any version, activate the BIOS, then reboot the system.	2.2(6c)A Resolved in 2.2(6e)A
CSCuv45173	When you upgrade C-series server firmware for C220-M4, C240-M4 to Cisco UCS Manager 2.2(6c), you will see the following critical alarm: `Board controller upgraded, manual a/c power cycle required on server x.`	The alarm seen is mistakenly categorized as a critical alarm. It does not impact the functionality of the server and can be ignored.	2.2(6d)C
CSCuw13352	If you set the Processor C6 Report to enabled in the BIOS policy, the system hangs during the OS boot process.	When configuring the Processor C6 Report in the BIOS policy, accept the default value of disabled.	2.2(6c)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuu78398	All blades running with the Storage Controller Firmware that does not support 4K native drives are showing the wrong virtual drive block size.	This issue has no known workaround.	2.2(6c)A
CSCuv18630	Cisco UCS B420 M3 servers with the firmware for UCSB-MRAID12G installed reports a nonfunctional Toshiba hard drive as Missing in Cisco UCS Manager.	This issue has no known workaround.	2.2(6c)A
CSCuv25760	On CPU 4830 and 4850, the P-state is not changing when running the linpack benchmark on Redhat, which results in the frequency not increasing.	This issue has no known workaround.	2.2(6c)A
CSCuv27475	The UCS B-Series Blade Servers include a version of Unified Extensible Firmware Interface (UEFI) that is affected by the vulnerabilities identified by the Common Vulnerability and Exposures (CVE) IDs: CVE-2014-8274.	This issue has no known workaround.	2.2(6c)A
CSCuv27587	The import configuration fails when call home is not configured while performing a backup operation. **Note** Call home is configured in the system where UCS Manager imports the configuration.	Configure call home before taking a backup.	2.2(6c)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuv38136	The platform might hang if there are any errors during the boot loader phase when in UEFI boot mode and using a Fibre Channel (FC) boot. Error conditions that require re-discovery/login for the FC LUN path during the BIOS boot phase, until the OS takes over, are currently not handled by VIC Oprom UEFI Driver. This results in a hang when the OS is being loaded by the BIOS using a VIC UEFI driver.	Shutdown and reboot the server.	2.2(6c)A
CSCuv59487	SPAN does not capture broadcast packets when you add vNIC as source.	Use the HIF port where the Virtual Network Interface (vEth) is bound as the SPAN source.	2.2(6c)A
CSCuv62162	The Power Technology token in UCS Manager BIOS policy has no effect on relevant CPU power performance option, such as EIST, Turbo Mode, P-States, and C-States.	Each setup option that is meant to be controlled by the Power Technology token should be set manually in UCS Manager.	2.2(6c)A
CSCuv76884	The Adaptor policies of dynamic vNICs created for a Global Service Profile (GSP) vNIC on UCS Manager are incorrect when there are two Dynamic vNIC policies with the same name created in different organization levels.	Change the Global Service Profile label to update the service profile vNICs. **Note** This might cause the server to reboot.	2.2(6c)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuv88433	UCS Manager displays a different sets of I2C data based on whether the data is from the master IOM or the slave IOM that is connected to the primary fabric. **Note** If UCS Manager primary is connected to the master IOM, the correct set of 12C data is collected.	There is no workaround for this issue.	2.2(6c)A
CSCuw10623	SBR firmware updates for servers with LSI9271-8i adapter appear to have a loss of datastore in the ESXi host.	There is no workaround for this issue.	2.2(6c)A
CSCuy98678	Cisco UCS 6296 fabric interconnect may crash unexpectedly with kernel panic, and impact any devices connected the fabric interconnect.	Reboot the fabric interconnect to restore connectivity.	2.2(6c)A Resolved in 2.2(8a)A
CSCuw55142	Cisco UCS B420M4 server with the UCSB-MRAID12G-HE no longer reports the following critical fault: `Controller 1 on server is inoperable. Reason: Device non-responsive`	There is no workaround for this issue.	2.2(6c)B Resolved in 2.2(6f)B, 2.2(7b)B

Open Caveats in Release 2.2(5c)

Open Caveats in Release 2.2(5c)

Table 60: Open Caveats in Release 2.2(5c)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCva27558	In scenarios such as traffic loops in external networks, a series of MAC add or delete operations may cause a missing MAC address in the software table, or in the hardware table for all the ASICs.	Avoid traffic loops in the external network. Once the problem is encountered, the MAC address can be manually cleared from the CLI to fix the issue. Example: `ESC-POD-0025-A(nxos)# clear mac address-table dynamic address 0050.56b2.4db2 vlan 205`	2.2(5c)A Resolved in 2.2(8c)A
CSCux59912	A Cisco UCS system with servers connected to a Cisco Nexus 2232 FEX experiences bladeAG cores that are displayed in the switch logs.	If this issue occurs, restart bladeAG through dplug or restart PMON.	2.2(5c)C Resolved in 2.2(8a)C
CSCuw13170	When auto-deploying the installation of ESX on Ivy Bridge-EX platforms, some platforms that enforce ACS violations strictly will generate a non-maskable interrupt (NMI), and the host OS may crash.	There is no known workaround.	2.2(5c)B Resolved in 2.2(5d)B

Open Caveats in Release 2.2(5b)

Open Caveats in Release 2.2(5b)

Table 61: Open Caveats in Release 2.2(5b)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuy01645	DIMM temperature readings are reported as NA when the temperature is 16 degree Celsius more than the previous reading. This results in missed temperature readings, which in turn results in Cisco UCS Manager generating thermal alerts.	This issue has no known workaround.	2.2(5b)B Resolved in 2.2(6i)B, 2.2(7c)B
CSCux96432	Discovery fails on UCS B420 M4 servers with a 2-CPU configuration and a Fusion IO card in adapter slot 3.	To resolve this issue, update the BIOS to version 2.2.6d.0 or later versions.	Resolved in 2.2(6g)B 2.2(5b)B
CSCux40478	When installing a Cisco B200 M3 blade server with a UCSB-MLOM-40G-01 40G VIC and either a UCSB-F-FIO-1300MP or a UCSB-F-1600MS ioMemory PCIe flash Mezzanine card, in a chassis with an N20-I6584 IOM, blade discovery fails with an “Invalid adapter-iocard combination” error.	When this issue occurs, remove the flash Mezzanine card to be able to continue installation.	2.2(5b)B Resolved in 2.2(6f)B

Open Caveats in Release 2.2(5a)

Open Caveats in Release 2.2(5a)

Table 62: Open Caveats in Release 2.2(5a)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvb08928	A fabric interconnect may reboot from a VLAN deletion due to a FWM hap reset.	Avoid deleting a VLAN.	2.2(5a)A Resolved in 2.2(8f)A
CSCuw44524	When using Cisco UCS Manager Release 2.2(5a), 2.2(5b), 2.2(5c) or 2.2(6c) for E7 v2 processors on the C460 M4, B260 M4, and B460 M4 servers, while you perform a clear CMOS BIOS operation, the following error may occur, which eventually causes the server to reboot or crash: `System Software event: Memory sensor, Uncorrectable ECC error, DIMM socket 1, Channel A, Memory Riser 2, Processor Socket 1. was asserted` **Note** This issue is specific to Cisco UCS Manager B and C server bundles.	When this issue occurs, downgrade to Cisco UCS Manager Release 2.2(4c). **Note** This issue will not be seen when using versions prior to Cisco UCS Manager release 2.2(5a), since support for both E7 v2 and v3 processors is available from Cisco UCS Manager release 2.2(5a).	2.2(5a)B 2.2(5a)C Resolved in 2.2(6e)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuv04436	Cisco UCS B200 M4 servers with the following CPUs may experience performance degradation: • E5-2667 v3 • E5-2643 v3 • E5-2640 v3 • E5-2637 v3 • E5-2630 v3 • E5-2630L v3 • E5-2623 v3 • E5-2620 v3 • E5-2609 v3	There is no workaround for this issue. See the Software Advisory. A patch will be released in July, 2015.	2.2(4b)B
CSCuu38206	If you disable and enable TXT several times, the state of TXT in the Cisco UCS Manager BIOS policy and the actual tboot state may get out of sync.	When this occurs, do the following: • Clear the CMOS • Re-apply the Cisco UCS Manager BIOS policy	2.2(5a)B
CSCuu58282	In Cisco UCS B420 M4 servers with UCSB-MRAID12G and UCSB-LSTOR-PT RAID controllers, in the rare event that Online Controller Reset (OCR) is triggered during normal I/Os on JBOD drives, excessive Fast Path IO failures may be seen after the controller is reset.	When this occurs, reboot the host.	2.2(5a)B Resolved in 2.2(5b)B
CSCuu35687	In Cisco UCS B420 M4 servers with UCSB-MRAID12G and UCSB-LSTOR-PT RAID controllers, the Fault/Locator LEDs for disks 3 and 4 are swapped.	This issue has no known workaround.	2.2(5a)B Resolved in 2.2(5b)B

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuu49909	If you disable TXT in the Cisco UCS Manager BIOS policy after installing ESX with TXT enabled, ESX becomes unresponsive and displays the following message: `Relocating modules and starting up the kernel....`	When this issue occurs, do one of the following: • Re-enable TXT • Re-flash BIOS	2.2(5a)B
CSCuu61885 CSCuu71563	When UCS C460 M4 servers with Intel® Haswell processors are in UCSM mode, if the boot order policy is configured to boot from SAN, and the network adapter connected to it is installed on any PCIe slot other than PCIe slot 4, the BIOS may not show the SAN boot device in the boot order, and the system may fail to boot from SAN. As a result of SAN boot failure, the system may become unresponsive at the end of the BIOS POST, or attempt to boot from other boot devices configured in the boot order policy. If the system is booted from some other boot device, for example, Local HDD, the SAN LUN will still be accessible and usable.	When this issue occurs, do the following: • Install the network adapter on PCIe slot 4 • Re-acknowledge the server • Re-configure the boot order policy • If the issue still persists, try rebooting the system a few times.	2.2(5a)C

Open Caveats in Release 2.2(4b)

Open Caveats in Release 2.2(4b)

Table 63: Open Caveats in Release 2.2(4b)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvg44307	Communication between two end hosts may fail within the same VLAN and fabric interconnect.	Reboot the IOM to recover from this condition.	2.2(4b)A Resolved in 2.2(8i)A
CSCvc46313	Remote operation from UCS Central no longer fails with the error message: `Global Service profile [org-root/org-GKDC/org-<name>/ls-SP_3260_03] can not be modified from UCS domain. Please make the changes from UCS Central that you are registered with.`	There is no known workaround. Contact TAC for assistance.	2.2(4b)A Resolved in 2.2(8g)A
CSCuu29425	Prior to RHEL 7.0, packets received on the native VLAN were properly processed by the driver and the OS. RHEL 7.0 and 7.1 introduced a regression that does not allow the ENIC driver to properly handle packets received on the native VLAN. These packets are reported by the ENIC driver as received on VLAN 0 and will not be properly processed by the network stack. In particular by software devices such as a bridge. RHEL 7.2 fixes this regression.	Go to https://access.redhat.com/announcements/2058583 to download and apply the RHEL 7.2 upstream patch. You can also apply the following two patches that RedHat applied to RHEL 7.2 to fix the issue. http://lists.openwall.net/netdev/2013/09/10/30 https://lists.linuxfoundation.org/pipermail/bridge/2015-July/009630.html	2.2(4b)B Resolved in 2.2(8c)B

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuw50361	While collecting IOM tech-support by using the show platform software satctrl global output from the IOM, the HIF/NIF interfaces of an IOM may flap due to SDP heartbeat timeout.	If you have encountered this SDP timeout during tech-support collection, take the following actions for any subsequent tech-support on the chassis that had been impacted: • If troubleshooting a blade or host level issue, specify the exact blade in question to only collect the CIMC and adapter logs. Note: The default chassis selection of CIMC ID: all will collect IOM logs as well. • If troubleshooting an IOM level issue, contact TAC for additional assistance.	2.2(4b)A Resolved in 2.2(8c)A
CSCuv32417	Cisco B200 M4 and B420 M4 blade servers that run on UEFI OS may reboot unexpectedly when BIOS POST is not marked as complete.	There is no workaround for this issue.	2.2(4b)B Resolved in 2.2(6e)B
CSCuw23829	When inserting a HDD into the final disk slot of a C240 M4 server with 8 supported slots for disks, Cisco UCS Manager may displays a additional disk in the 9th slot, which is non-existent.	This error has no workaround. It does not affect any functionality. All the HDD operations can still be performed on the HDD shown on the final slot. However, any operation or configuration attempted on the invalid HDD will result in an error.	2.2(4b)A Resolved in 2.2(6e)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuv20999	When Cisco UCS Manager is managed by Cisco UCS Central, and there is a global service profile associated with a blade server, global VLANs cannot be assigned to a particular uplink interface through Cisco UCS Manager (**VLAN Uplink Manager** > **VLANs** > **VLAN Manager**), and the following error message is displayed: `Global Service Profile[xxxxx] cannot be modified from UCS domain. Please make the changes from UCS Central that you are registered with.`	When this error occurs, do the following: 1. Disassociate all the service profiles that would use the VLANs. 2. Manually configure disjoint layer 2 on Cisco UCS Manager. 3. Associate the service profiles back to the blade servers.	2.2(4b)A Resolved in 2.2(5d)A

CSCuw50417	After upgrading the BIOS of Cisco UCS B200 M3 servers to any release between 2.2(4b) and 2.2(5c), the OS may randomly report the following messages in the /var/log/boot.gz file of the OS if the OS boot time is exceptionally slow:
	`Initializing Power Management ...`
	`Power: 2568: No supported CPU power management technology detected`
	`Intel Enhanced SpeedStep is supported but disabled in BIOS`
		When this error occurs, it disables the OS PM capability, but has no known workaround to resolve it.	2.2(4b)B
			Resolved in 2.2(5d)B

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuu89283	Service profile association fails and displays the following message: `Controller does not support non-default virtual drive properties` This happens when you modify virtual drive policy attributes, such as read-policy, write-policy, and cache-policy, for a rack server with a UCSC-MRAID12G storage controller that has LUNS managed through storage profiles.	There is no known workaround for this issue.	2.2(4b)A Resolved in 2.2(5c)A
CSCuv00089	After upgrading the Fabric Interconnect to Cisco UCS Manager Release 2.2(4) or 2.2(5), systems that have OS-based NIC teaming configured as Active-Standby will experience network connectivity issues. This is because the MAC addresses of teamed interfaces are learned statically on both FI server ports. **Note** Network connectivity issues still occur when you upgrade the FI to Cisco UCS Manager Release 2.2(4), although it is resolved when you upgrade to Release 2.2(5).	When this issue occurs, do one of the following: • Change NIC teaming to Active-Active configuration. • Disable the slave or backup interface from OS. There will be no redundancy with this option, and it can restore network connectivity until you can implement fabric failover configuration. • Instead of OS-based NIC teaming, use a single vNIC in the service profile and enable fabric failover for it. **Note** This configuration change requires server reboot.	2.2(4b)A Resolved in 2.2(5c)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuv13545	If Cisco UCS Manager is registered with Cisco UCS Central, and the service profile refers to a global host firmware pack policy, UCSM downloads images instead of skipping it during shallow discovery.	There is no known workaround for this issue.	2.2(4b)A Resolved in 2.2(5c)A

CSCuv29668	When using Cisco UCS 6100 Series Fabric Interconnects with Cisco UCS 2100 IOMs, some blade servers with two Cisco UCS M81KR VIC adapters fail discovery after updating Cisco UCS Manager to Release 2.2.(4b) and later releases, or to Release 2.2(5a). The second adapter causes the discovery failure.
	UCS Manager could display several errors including the following:
	`sendsamedmeadapterinfo: identify failed`
	`adapter: repo lookup failed`
		Downgrade UCS Manager to a release earlier than Release 2.2(4b).	2.2(4b)A
			Resolved in 2.2(5b)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuv04436	Cisco UCS B200 M4 servers with the following CPUs may experience performance degradation: • E5-2667 v3 • E5-2643 v3 • E5-2640 v3 • E5-2637 v3 • E5-2630 v3 • E5-2630L v3 • E5-2623 v3 • E5-2620 v3 • E5-2609 v3	There is no workaround for this issue. See the Software Advisory. A patch will be released in July, 2015.	2.2(4b)B
CSCut54652	If the rack server is using UCSC-PCIE-C10T-02 or UCSC-MLOM-C10T-02 adapters, during service profile association, firmware upgrade on any third-party Converged Network Adapter (CNA) fails with the following error: `Unable to find VNIC Device`	When this occurs, do the following: 1. Remove all vHBAs and vNICs from the service profile that is placed on UCSC-MLOM-C10T-02 or UCSC-PCIE-C10T-02. **Note** Re-association triggers automatically and the firmware upgrade on third-party CNAs will succeed. 2. To the service profile, add the vHBAs and VNICs that were removed in step 1.	2.2(4b)A Resolved in 2.2(5a)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuu53920	In a Cisco UCS B460 M4 server, service profile association fails when virtual drive creation is attempted by using a storage profile on a slave RAID controller.	This issue has no known workaround.	2.2(4b)A Resolved in 2.2(5a)A
CSCut53878	When port profiles do not have any VLANs and both Fabric Interconnects are rebooted, STP cores are observed.	To avoid this, during port profile creation, ensure that each port profile has at least one VLAN.	2.2(4b)A
CSCuu52001	In a C-Series rack server with an external RAID controller, service profile association fails at 78% with the following error message: `cannot support multiple scsi controllers`	Remove the external RAID controller, and the service profile association will complete successfully.	2.2(4b)C Resolved in 2.2(5a)A
CSCuu37369	A storage profile can be created in the main organization within Cisco UCS Manager, but it cannot be created through a sub-organization.	Use the Cisco UCS Manager CLI to create a storage profile in a sub-organization: **1.** scope org **2.** create storage-profile name **3.** commit-buffer You can also create a storage profile within the sub-organization service profile during service profile creation.	2.2(4b)A Resolved in 2.2(5a)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuu42945	Service profiles created from service profile templates with local storage profiles fail association with the following error: `Server unavailable, there are not enough resources overall, incomplete LUN configuration.`	When this occurs, modify the description of service profile template.	2.2(4b)A Resolved in 2.2(5a)A
CSCuu65128	If you configure more than 64 vNICs (excluding dynamic vNICs) on a single server, the Fabric Interconnect reboots continuously due to an LLDP core.	Do not configure more than 64 static vNICs on a single server (excluding dynamic vNICs)	2.2(4b)A Resolved in 2.2(5a)A
CSCus73395	If the discovery policy is configured as Platform-Max, and all links are not connected and acknowledged, servers are not discovered on first installation with import all backup configuration.	When this occurs, reacknowledge the chassis to start discovering the servers.	2.2(4b)A
CSCuo62019	When adding or deleting multiple VLANs for a large number of port profiles as part of a single operation, the DME might restart.	When this occurs, apply each addition or deletion as separate operations instead of as a bulk operation.	2.2(1b)A
CSCut72773	Installation of ESXi 5.5 U2 fails through PXE boot on Cisco UCS M4 servers in UEFI boot mode.	This issue has no known workaround. Alternate options include: • Use the boot script from ESXi 6.0 Use the legacy BIOS mode for PXE installation	2.2(4b)B

Defect ID	Symptom	Workaround	First Bundle Affected
CSCut35123	After high availability failover, you may see chassis-seeprom local IO failure with the following message: `Warning: there are pending SEEPROM errors on one or more devices, failover may not complete.`	When this occurs, reset the power supply unit.	2.2(4b)A Resolved in 2.2(6c)A
CSCus71522	Changes made to the user-defined flow record definitions for NetFlow are not updated and propagated to the vNIC that is already using the existing flow record definition.	When this occurs, remove the policy from the interface and reapply.	2.2(4b)A
CSCut96983	For LUNs that are created by using the local disk configuration policy, the option to add UEFI boot parameters is not enabled. Hence, local LUN boot fails for UEFI after service profile migration.	For UEFI boot from local LUN, use LUNs that are created by using storage profiles.	2.2(4b)A
CSCup43526	On a scale Cisco UCS system, creation and download of the technical support file from the Cisco UCS Manager GUI times out with a timeout message.	Even though the timeout message appears in the Cisco UCS Manager GUI, the technical support file is created and saved locally.	2.2(1b)A
CSCut78943	When a service profile is associated to a server with a Cisco UCS VIC 1340 or VIC 1380 adapter, the actual order of vNICs and vHBAs does not reflect the configured order.	In Cisco UCS Manager, specify the vNIC/vHBA placement order manually using the following steps:	2.2(3c)A Resolved in 2.2(6c)A

Defect ID	Symptom	Workaround	First Bundle Affected
		1. Expand **Service_Profile_Name** > **vNICs**. 2. In the Work pane, click the **Network** tab. 3. In the Actions area, click **Modify vNIC/vHBA Placement**. In the **Modify vNIC/vHBA Placement** dialog box that appears, do the following: a. Choose Specify Manually from the Select Placement drop-down list. b. Explicitly assign the vNICs and vHBAs to the vCons. c. In the list of Specific Virtual Network Interfaces, select the vNICs or vHBAs that you have newly assigned to the vCons, and set Admin Host Port for these vNICs or vHBAs as 2. 4. Save the configuration.	

Defect ID	Symptom	Workaround	First Bundle Affected
CSCva72096	Cisco UCS servers running Intel E5 Xeon v4 CPUs crashed with a signature pointing to internal parity errors, page fault, general detect, or undefined opcode exceptions.	This issue has no known workaround.	2.2(4b)B Resolved in 2.2(7e)B, 2.2(8b)B

Open Caveats in Release 2.2(3k)

Open Caveats in Release 2.2(3k)

Table 64: Open Caveats in Release 2.2(3k)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvb78971	When attempting the auto-install of UCS Manager, the fabric interconnect upgrade may fail when the /var/tmp usage exceeds 10%.	There is no workaround for this issue.	2.2(3k)A Resolved in 2.2(3l)A, 2.2(8f)A

Open Caveats in Release 2.2(3j)

Open Caveats in Release 2.2(3j)

Table 65: Open Caveats in Release 2.2(3j)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuv97713	After upgrading Cisco UCS Manager, in rare cases, the IOM may core in the sysmgr process leading to IOM reboot.	There is no workaround for this issue.	2.2(3j)A Resolved in 2.2(3k)A, 2.2(6g)A

Open Caveats in Release 2.2(3h)

Open Caveats in Release 2.2(3h)

Table 66: Open Caveats in Release 2.2(3h)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCux10203	When you decommission a C-Series server after it was discovered in direct attached configuration, and the direct attached switch port was changed from Ethernet to FC mode, the following error message may appear: `Warning : if_index 0x1a01a000[Ethx/x] does not exists in VLAN database#ERROR`	When this issue occurs, switch the ports back to Ethernet mode from FC mode and allow the server decommission to complete.	2.2(3h)A Resolved in 2.2(3j)A, 2.2(6e)A
CSCuw59409	When you upgrade a directly connected C-Series rack server without decommissioning, and connect the server to FI port, you may experience a DME crash issue.	Contact TAC to decommission the rack server from the back end.	2.2(3h)A Resolved in 2.2(3j)A, 2.2(6e)A
CSCuw84010	Integrated C-Series rack servers with Seagate drives fail association when using the host firmware policy in a service profile.	Do one of the following: • Remove the C-Series rack server from UCSM integration and manually updating the server with HUU. Remove the host firmware package from the service profile. Remove the Seagate disks from the C-Series servers and place them in B-Series servers.	2.2(3h)A Resolved in 2.2(3j)A, 2.2(6e)A

Open Caveats in Release 2.2(3g)

Open Caveats in Release 2.2(3g)

Table 67: Open Caveats in Release 2.2(3g)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuv46749	When using Cisco B200 M4 blade servers with the UCSB-MRAID12G storage controller, the following random transient alerts or faults are incorrectly reported, and these alerts or faults get cleared in 30 to 40 secs: • Critical Fault [F1004] Controller Inoperable, Reason: Device reported corrupt data • Critical Fault [F1004] Controller Inoperable, Reason: Device non-responsive **Note** When a Storage Controller device is non-responsive, the virtual drives and local disks for this controller are also reported as Inoperable as a result.	No known workaround.	2.2(3g)B Resolved in 2.2(6f)B
CSCuv51214	Messages log overfilled with BMC is suspecting that palo is in boot block. Leaving I2C bus alone. messages.	No known workaround.	2.2(3g) Resolved in 2.2 (6c)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuv28540	When you run Cisco UCS Manager Releases between 2.2(1) and 2.2(3) with catalog versions 2.2(4b)T or 2.2(5a)T, SAN boot fails on servers where the boot vHBAs are placed on a VIC. This is because the VIC PCI slot ID displays N/A in the UCSM inventory. **Note** This issue is resolved when you use catalog version 2.2(5b)T, but still occurs with catalog versions 2.2(4b)T and 2.2(5a)T.	Downgrade the catalog version to the corresponding Cisco UCS Manager release and re-acknowledge the rack server.	2.2(3g)A Resolved in 2.2(5c)A with catalog version 2.2(5b)T

Open Caveats in Release 2.2(3f)

Open Caveats in Release 2.2(3f)

Table 68: Open Caveats in Release 2.2(3f)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCva14937	M4 blades installed with SD cards instead of a hard disk may halt at 'Local Drive' for automated deployments with the following boot policy: Boot Policy • CD/DVD • Local Drive • Network Adapter (PXE)	There is no known workaround.	2.2(3f)B Resolved in 2.2(8g)B

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuu66595	An error prevented multiple backups to the same host.	Delete the previously created configuration entry from Backup operations table.	2.2(3f)A Resolved in 2.2(3l)A
CSCuy79306	When Cisco UCS C-Series servers with VIC 1225 or VIC 1227 are directly connected to Cisco Nexus 9000 switches, after making a large change on a switch, ports may flap or show as down on the switch but up on the server.	When this issue occurs, do one of the following: • Shut/no-shut the port. • Reseat the cable. • Shutdown then startup the server. • Reset the VIC card Another workaround is to change the debounce timer to 3 seconds: `conf ; interface eth x/y ; link debounce timer 3000`	2.2(3f)C Resolved in 2.2(8c)B
CSCux05389	Occasional VSAN misconfiguration occurs after upgrading to release 2.2(3f) and rebooting the subordinate fabric interconnect.	When this issue occurs, do one of the following: • Change the VSAN on the HBA to a VSAN that is not in use, and then change it back to the correct VSAN. • Revert to the previous release.	2.2(3f)A Resolved in 2.2(7b)A
CSCuv89839	When the fabric interconnect is in switch mode with direct attached storage, and its FC uplinks to the direct attached storage are up, these FC uplinks do not allow traffic to pass.	When this issue occurs, run the shut and no shut commands on the affected ports, for example, vfc or FC uplink.	2.2(3f)A Resolved in 2.2(6g)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuu16791	The Firmware Auto Sync Server Policy is Auto Acknowledge by default. This setting attempts to push the default Host Firmware Package firmware in to newly attached blades/rack-servers.	Change the Auto Sync Server Policy option to No actions.	2.2(3f)A
CSCuu60867	Unable to discover UCS C240 M3 servers with dual RAID controllers through Cisco UCS Manager.	When this issue occurs, remove one of the two RAID controllers and re-discover the server.	2.2(3f)A Resolved in 2.2(5c)A

Open Caveats in Release 2.2(3d)

Open Caveats in Release 2.2(3d)

Table 69: Open Caveats in Release 2.2(3d)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCva31113	After a Fabric Interconnect reboot, the FI does not fully boot and become network accessible. The Serial Console connection to the FI may show a "loader" prompt or show initial configuration prompts.	In most cases the underlying file system corruption can be fixed by booting into the kickstart image and running a file system check. There is no guaranteed preventative workaround. Although corruption may still occur, it is recommended to use the pre-upgrade package to send proper SSD shutdown commands prior to reboot. A pre-upgrade package containing a script and a kernel module was developed for 62xx Fabric Interconnects running 2.2(x) firmware to ensure proper SSD shutdown prior to the reboot required during the upgrade process. With this deployed, the risk to run into a file system corruption issue during reboot is reduced, however not eliminated. Please contact Cisco TAC for assistance with recovery or the pre-upgrade script. **Note** The pre-upgrade script will NOT work on 61xx FIs or 2.1(x) UCS firmware.	2.2(3d)A Resolved in 2.2(8i)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCva04106	Removing a SAN port channel member may cause SAN ports to go down.	When this issue occurs, do the following: **1.** Disable the member interface in UCSM before removing it from SAN Port Channel. **2.** Configure the PO and member ports in Trunking mode.	2.2(3d)A Resolved in 2.2(8a)A

CSCuu40978	If a large number of syslog messages are generated, the syslog file may fill the Fabric Interconnect file system and prevent it from being written into.	If you are unable to write to the filesystem, use the following commands on the Fabric Interconnect to verify whether the issue is caused by the syslog messages file:
		`connect nxos a | b show system internal flash | grep root`
		Note In the output, check for close to 100 percent usage
		`show system internal dir /var/log/external`
		Note In the output, note the size of the messages file in bytes
			2.2(3d)A
			Resolved in 2.2(3k)A, 2.2(6i)A, 2.2(7d)A, 2.2(8b)A

Defect ID	Symptom	Workaround	First Bundle Affected
		If the file is close to 100 MB: From **Admin** > **Faults, Events and Audit Log** > **Syslog**, reduce the size of the local syslog file. You can increase the size of this file later. Longer term workaround: Ensure that the severity for the local file is set to **Critical**. If you still see significant growth of the file even after reducing the size of the local syslog file once, you either will need to repeat the steps or disable the syslog file entirely and use a remote destination.	
CSCuv31912	Cisco UCS Manager iptables are duplicating rules in the FORWARD table.	Reboot the fabric interconnect to clear the entries. If the duplicate entries are in the thousands, or if there are connectivity issues to Cisco UCS Manager because of missing rules in the INPUT tables, contact TAC for help with the workaround.	2.2(3d)A Resolved in 2.2(3j)A, 2.2(6c)A, 2.2(8a)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuv06504	The **svc_sam_dme** process crashes during steady state of operation when a database(db) corruption is detected primarily on the subordinate fabric interconnect. When the subordinate fabric interconnect detects a nvram or flash db corruption, it initiates a self-healing mechanism to rectify the sqlite db. After the sqlite db on the subordinate is rectified, the **svc_sam_dme** reloads the db and during this reload it sometimes crashes.	There is no workaround. The system recovers on its own after svc_sam_dme restarts.	2.2(3d)A Resolved in 2.2(3j)A, 2.2(6c)A

CSCus73196	Installation of ESXi 5.5 Update 2 and later updates, or ESXi 6.0 and later updates on the FlexFlash of a Cisco UCS B200 M4 server fails with the following error:
	`partedUtil failed with message: Error: Can't have a partition outside the disk!`
	`Unable to read partition table for device`
		To avoid this issue, disk scrub the FlexFlash before installing an Operating System.	2.2(3d)B

Defect ID	Symptom	Workaround	First Bundle Affected

CSCur99740	While upgrading or downgrading the Fabric Interconnect image on the Cisco 6100 series, you may see the following symptoms:
	• The Fabric Interconnect image upgrade fails while upgrading from Cisco UCS Manager Release 2.2(3d) to Cisco UCS Manager Release 2.2(3e) and higher releases.
	• Auto-install fails during Fabric Interconnect image upgrade from Cisco UCS Manager Release 2.2(3d) to Cisco UCS Manager Release 2.2(3e) and higher releases.
	• The Fabric Interconnect image downgrade fails while downgrading from Cisco UCS Manager Release 2.2(3d) to all lower releases.
	• Auto-install fails during Fabric Interconnect image downgrade from Cisco UCS Manager Release 2.2(3d) to all lower releases.
		To recover from upgrade or downgrade failure, reboot using the Cisco UCS Manager CLI, or power cycle the Cisco 6100 series FI:
		Example:
		`UCS-A# connect local-mgmt`
		`UCS-A(local-mgmt)# reboot`
		To recover from Auto-install failure:
		• Reboot using the Cisco UCS Manager CLI, or power cycle the subordinate FI.
		Directly upgrade or downgrade the primary FI.
		Reboot using the Cisco UCS Manager CLI, or power cycle the primary FI.
			2.2(3d)A
			Resolved in 2.2(3e)A.

CSCus76125	Global service profile will not resolve the LAN ping group even when the ping group is created in Cisco UCS Manager.	This isssue has no workaround. Please contact Cisco TAC for help with this issue.	Resolved in 2.2(3k)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuz67284	When installing the ESXi 5.5 U2 custom ISO to FlexFLash, the partedUtil fails with the following error message: “Can't have a partition outside the disk! Unable to read partition table for device.	Scrub the FlexFlash drives to install the ISO without any issues.	2.2(3d)

Open Caveats in Release 2.2(3c)

Open Caveats in Release 2.2(3c)

Table 70: Open Caveats in Release 2.2(3c)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCus93431	Adding other storage, such as a local disk or a USB to a SAN boot only policy deletes the SAN boot policy from Cisco UCS Manager.	Modify the boot policy description, and save the boot policy again to Cisco UCS Manager.	2.2(3c)A Resolved in 2.2(3j)A, 2.2(6c)A
CSCus81832	When a Cisco UCS VIC 1340 or VIC 1380 adapter is used with a Sandy Bridge CPU in a Cisco UCS B420 or UCS B200 M3 server, the server hangs. This causes the KVM console window to become unresponsive and the installation of Red Hat Enterprise Linux 6.5 or 7.0 is not completed.	When this issue occurs, change the adapter to Cisco UCS VIC 1240 or VIC 1280.	2.2(3c)B Resolved in 2.2(4b)B.
CSCur70034	Service Profiles with a common VLAN name configured on one of the vNICs fail with the following error: Incorrect VLAN configuration on one of the VNICs.	To resolve this issue, either delete the local-vlan with the same vlan-ID on Fabric A, or modify the service-profile vNIC to point to the Fabric-A vlan name.	2.2(3c)A Resolved in 2.2(3e)A.
CSCut45598	Kernel Panic on Fabric Interconnect.	None.	2.2(3c)A Resolved in 2.2(3g)A

Open Caveats in Release 2.2(3b)

Open Caveats in Release 2.2(3b)

Table 71: Open Caveats in Release 2.2(3b)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuz74973	When you use a B200 M4 server with a UCSB-MRAID12G SAS RAID controller and a CPLD firmware version earlier than version 05D, the B200 M4 server powers off unexpectedly. The OBFL displays the following log message: `[platform_power_state_irq_handler]: 18: VDD_PWR_GOOD: Deasserted`	If this issue occurs, upgrade the infrastructure and server firmware to Cisco UCS Manager Release 2.2(7b) or later releases. **Note** Both infrastructure and server firmware must be upgraded. If the server firmware is upgraded to a fixed release earlier than the infrastructure firmware, do one of the following after the infrastructure firmware is upgraded to the fixed release. • Re-acknowledge the server • Decommission and then acknowledge the server This is required for the correct server firmware component to upgrade and prevent the issue.	2.2(3b)B Resolved in 2.2(7b)B

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuw16950	The FSM does not handle failure scenarios such as domain name resolution failures. FSM failure in such scenarios can trigger the addition of duplicate entries in IP tables. The longer the uptime after a trigger condition, the more the duplicate entries.	To prevent known triggers for this issue, resolve any Cisco UCS Manager faults or issues that are related to external hosts or services such as NTP and DNS. When this issue occurs, contact TAC to perform the workaround described in CSCuv31912. After the temporary workaround has been deployed, it is still highly advised to resolve Cisco UCS Manager faults or issues that are related to external hosts or services. If this is not done, the issue may reoccur.	2.2(3b)A Resolved in 2.2(8a)A
CSCux85580	Fabric Interconnect cores will be seen on IGMP.	This issue has no known workarounds.	2.2(3b)A Resolved in 2.2(7b)A

Defect ID	Symptom	Workaround	First Bundle Affected

CSCux71937	The CPU utilization always displays 100 percent for the kernel in the output of the show system resources command. This could happen if the system had been up for a very long time (more than 200 days, but this time-frame could vary):
	`FI(nx-os)# show system resources`
	`Load average: 1 minute: 0.50 5 minutes: 0.71 15 minutes: 1.04`
	`Processes : 563 total, 3 running`
	`CPU states : 0.0% user, 100.0% kernel, 0.0% idle`
	`Memory usage: 3490164K total, 3140304K used, 349860K free`
		If this issue occurs, reload to reset the memory.	2.2(3b)A
			Resolved in 2.2(3j)A, 2.2(6f)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuu33864	When upgrading to a Cisco UCS Manager 2.2 release earlier than Release 2.2(6c), the fabric interconnect may become unresponsive at the loader prompt and not boot correctly. Various error messages may also be displayed.		2.2(3b)A Resolved in 2.2(6c)A, 3.1(1e), 3.1(2b)

Defect ID	Symptom	Workaround	First Bundle Affected
		Load a kickstart image either from the bootflash or through tftp. If the drive is still accessible, copy the debug plugin to it and load it. If the drive is no longer accessible, run the 'init system' command to re-initialize the SSD. If the drive is still accessible it may be possible to repair the file system corruption from the Linux shell as follows: **1.** unmount all partitions, /dev/sda3 .. /dev/sda9. You might also have to unmount /dev/mtdblock3 prior to being able to unmount /dev/sda7. **2.** run 'e2fsck -n -f /dev/sdaX' for X = {3, .., 9} **3.** Based on the number of errors, run 'e2fsck -y /dev/sdaX', X = {3, .., 9}, to attempt having the system repair the errors. It is recommended to copy critical data back to the SSD because data on disk could still be corrupted even after file system corruption has been fixed. Alternatively, you can run the init-system script to reinitialize the SSD. **Note** This can take a while depending on the size of the drive.	

Defect ID	Symptom	Workaround	First Bundle Affected
CSCut88909	When trying to map a Virtual Media, KVM becomes unresponsive. Map CD/DVD, Map Removable Disk, and Map Floppy Options are not displayed.	Do one of the following: 1. Eject the Optical Drive on the computer used to launch UCSM 2. Keep a CD/DVD in the Optical Drive. 3. Use a computer with no Optical Drive.	2.2(3b) Resolved in 2.2(6c)
CSCuu15465	If the version of board controller on a UCS B200 M4 server is higher than the version in the Host Firmware Pack, Cisco UCS Manager tries to downgrade firmware of board controllers on the servers. This power cycles the servers.	This issue has no known workaround.	2.2(3b)A Resolved in 2.2(3h)A
CSCuq74763	On Windows 2012 hypervisors, vmNICs configured with NVGRE network virtualization fail to initiate network traffic when NVGRE NIC task offloads is enabled. **Note** Installing patch KB2779768 resolves the issue for ping operation but does not resolve the issue for TCP/UDP traffic.	To use NVGRE NIC task offload feature, upgrade the hypervisor to Windows 2012 R2. Alternatively, disable the NVGRE task offload feature using Cisco UCS Manager or in the hypervisor while using Windows 2012.	2.2(3a)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuq88436	XML Parsing Error due to multiple jbod diskState attributes is incorrectly specified when a server with two or more local disks is configured with No RAID disk config policy.	This issue has no known workaround.	2.2(3b)A
CSCuq95926	If you unplug the primary management cable when the HA is not complete, the Cisco UCS FI HA status remains in “switchover in progress”.	Restart the primary DME using the pkill dme command, or reboot the FI.	2.2(2c)B
CSCup46033	On a FI with a GEM module installed, the total default quantity of licenses does not match the total quantity of licenses available by default.	This issue has no known workaround.	2.1(1f)A
CSCuq51890	entPhysicalDescr is returning the wrong getnext values during SNMPwalk.	Perform an SNMPwalk of 1.3.6.1.2.1.47.1.1.1.1.2.1 followed by 1.3.6.1.2.1.47.1.1.1.1.2.24 to get the remaining information.	2.2(2c)A
CSCus97608	Faults in Cisco UCS Manager such as “error accessing shared-storage” and timeout/failover warning within the “show cluster extended-state” are displayed when several devices in several chassis are reporting EBUSY within the I2C logs.	This issue has no known workaround.	Resolved in 2.2(3g)A
CSCut02769	While performing a dbsync between Cisco UCS Fabric Interconnects, the Cisco UCS database copies all the files, and just copies the required files.	This issue has no workaround.	Resolved in 2.2(3g)A

Open Caveats in Release 2.2(3a)

Open Caveats in Release 2.2(3a)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCux41398	UCS Manager includes a version of OpenSSL that is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) IDs: CVE-2015-3193, CVE-2015-3194, CVE-2015-3195, CVE-2015-3196 and CVE-2015-1794	There is no known workaround.	2.2(3a)B Resolved in 2.2(8i)B
CSCuq57142	In a port channel universe, the following may occur: • A port channel ID may sometimes not be released after use. This could eventually lead to the universe of port channel IDs being empty, and no port channel IDs being available for use. • After an upgrade, power loss, FI reboot or failover, the empty port channel universe is incorrectly interpreted as a new installation, and repopulated. This leads to duplicate port channel ID allocation when a server is attached to the FI, or when a server is re-acknowledged.	If this issue occurs: 1. Upgrade to a version of Cisco UCS Manager that fixes the port channel universe **Note** Upgrading Cisco UCS Manager does not fix pre-existing PC ID collisions, but prevents new PC ID collisions 2. Identify servers that have port channel ID collisions 3. Re-acknowledge servers that have a port channel ID collision	2.2(3a)A Resolved in 2.2(3k)A, 2.2(6i)A, 2.2(7c)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuy62783	In a UCS setup with a VIC 13xx adapter on blade servers or rack-mount servers with Microsoft Windows OS, the server or VIC adapter may become unresponsive after running IO across network file systems. As a result, the vNICs are disconnected from the OS, which leads to connectivity loss until server reboot. In the case of iSCSI booted systems, this may result in a 0x7B INACCESSIBLE_BOOT_DEVICE BSOD.	If this issue occurs, do the following: • Reboot the server as an immediate fix • Disable TSO as a long-term workaround until the firmware can be updated	2.2(3a)B Resolved in 2.2(6i)B, 2.2(7c)B

CSCuw44595	DIMMs with correctable ECC errors are marked Inoperable or Degraded even though correctable errors do not affect normal system operation.	For Cisco UCS Manager Release 2.2(1a) and later versions, clear the error messages with the following CLI commands:
		`scope server x/y`
		`reset-all-memory-errors`
		For Cisco UCS Manager Release 2.1(x), this example shows how to enter the DIMM mode for server 1/1 to reset-errors on a DIMM module 2 in memory-array 1:
		`UCS-A # scope server 1/1`
		`UCS-A /chassis/server # scope memory-array 1`
		`UCS-A /chassis/server/memory-array # scope dimm 2`
		`UCS-A /chassis/server/memory-array/ dimm # reset-errors`
			2.2(3a)A
			Resolved in 2.2(3k)A, 2.2(6i)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCux68679	When a UCS B460 M4 server is configured with Fusion IO cards installed in same mezzanine slot of the master and slave blades, actions such as Cisco UCS Manager upgrade, cluster failover, fabric interconnect reboot trigger server reboot.	To avoid this issue, install the Fusion IO card only in the master blade.	2.2(3a)A Resolved in 2.2(3k)A, 2.2(6g)A
CSCut10525	The FlexFlash firmware version is not updating and the FFCH_ERROR_OLD_ FIRMWARE_RUNNING is displaying in the fault summary after you update the UCS B200 M4 server firmware using Cisco UCS Manager Release 2.2(4b).	Reset the FlexFlash Controller manually to remove the error.	2.2(3a)B Resolved 2.2(3j)B
CSCuv72975	When upgrading the Cisco UCS Manager infrastructure bundle and using VIC-1340 or VIC-1380, the backplane port of the IOM and VIC goes down.	There is no known workaround.	2.2(3a)B Resolved in 2.2(3j)B
CSCuw78688	When the FI is rebooted or UCS Manager is activated to a new version and the DME database has a corrupted entry, you may see one of the following issues: • FI ports will be in unconfigured state • No service profiles, templates, policies or pools will display in UCS Manager GUI or CLI.	There is no known workaround. If UCS Manager has lost configuration, you can reimport the configuration using the all-config backup file. Contact Cisco TAC for more assistance.	2.2(3a)A Resolved in 2.2(6e)A, 2.2(3j)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCus55944	In a Cisco UCS Manager configuration with a C260 rack-mount server and two adapters, adding a VLAN to a vNIC on an service profile template immediately reboots the rack server that is associated with the inherited service profile.	**1.** Run the show detail command for both the adapters. **2.** Note the managing instance of both the adapters and the roles of the fabric interconnects-primary and secondary. **3.** Shut down the host-facing port from FI-A, which is connected to the specified server. **4.** Wait 5 minutes. **5.** Repeat Step 1 and ensure that the managing instance of both the adapters is the subordinate FI. **6.** Apply the service profile configuration change. The server reboots. The activation status of both adapters displays **Ready**. Any subsequent service profile configuration change will not result in a reboot unless the configuration itself requires a reboot.	2.2(3a)A Resolved in 2.2(3j)A, 2.2(4b)A
CSCur79257	When Cisco UCS Manager is configured as fc-uplink port-channel, and is being upgraded, the FSM fails and the vLANs are not added to FI B uplinks.	When this issue occurs, reboot the fabric interconnect.	

Defect ID	Symptom	Workaround	First Bundle Affected
CSCut37134	Cisco UCS B200 M4 servers running ESXi 5.5 will crash intermittently when booting locally.	**1.** Remove the lsi-mr3 RAID Controller driver and reboot **2.** Re-deploy ESXi with the latest ISO available.	
CSCup45804	VXLAN offload is enabled. Throughput is reduced because of two-way traffic between VMs.	This issue has no known workaround.	2.2(3a)A
CSCuo11544	In some cases, NicAG gets stuck when getting events from adapter when that adapter is busy performing other tasks.	To work around this issue, perform one of the following options: • Check for servers that are stuck in discovery, association, or disassociation state and, if found, decommission them. Then confirm that firmware update on adapters succeeds. • Instead of performing adapter firmware updates on multiple servers, perform a firmware update on servers in batches.	2.2(3a)B
CSCuq09577	In some cases, a system running a 6100 FI setup with a large number of rack servers becomes unresponsive due to a high number of error messages overfilling the Cisco UCS Manager log file when an insufficient number of FEX/IOM uplinks are configured.	Make sure a sufficient number of IOM/FEX uplinks are configured so that vNICs configured on each service profile do not exceed the limit.	2.2(2c)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuq14172	Windows 2012 and Windows 2012R2 systems hang (boot and installation) when TXT is enabled via BIOS setup.	This issue has no known workaround. Disable TXT and reboot.	2.2(2a)B
CSCuq28367	Host continuously reboots if scriptable vMedia mount fails and the same device type is also configured in boot policy.	Uncheck to disable the “Retry on mount fail” option in scriptable vMedia policy.	2.2(3a)A
CSCuq33306	SAN boot with Emulex adapter fails with the first vHBA created when creating a Cisco UCS Manager service profile boot policy to boot from SAN LUN from the first vHBA.	Use the second vHBA for booting and map boot targets to the second vHBA in the Emulex adapter.	2.2(3a)A
CSCuq44049	In rare cases, when adding SD cards dynamically (without powering down server) to a server without SD cards or when dynamically adding one SD card to a server with only one SD card, the server gets stuck in sync mode and disconnects existing drives accessed by host from an SD card.	To avoid potential data loss, first disable HOST VD access (from WEB UI or CLI) if VD access is enabled. Then, after confirming each SD card is plugged in properly, execute reset of the flex flash controller (from WEB UI or CLI).	2.0(3b)A
CSCuq63592	In some cases, blade association fails on servers with Cisco UCS VIC 1340 or Cisco UCS VIC 1380 adapters when some vHBAs are placed manually on Host Port 1 or Host Port 2 and some are placed by system when Desired Host Port is set to ‘ANY.’	Place all vHBAs manually on host ports 1/2 or allow system to place all vHBAs.	2.2(3a)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuq64931	Blades with Cisco UCS VIC 1340 or Cisco UCS VIC 1380 adapters fail remote OS boots when SRIOV vNICs are placed on first host port and static vNICs (PXE, iSCSI, or vHBA) are placed on second host port.	Place the SRIOV vNICs on the second host port manually via GUI or CLI options to set host port when configuring service profile.	2.2(3a)A
CSCuq81262	If anonymous reporting (AR) is enabled after upgrading Cisco UCS Manager to release 2.2(3a) in an environment specifically configured with VMs that use VM-FEX on any hypervisor, then Cisco UCS Manager becomes unresponsive after seven days when VM-related data collection begins.	Disable AR feature in Cisco UCS Manager if running any VMs that use VM-FEX on any hypervisor. (The AR feature is disabled by default.) If this issue (with AR enabled) is encountered, contact Cisco TAC for solution.	2.2(3a)A
CSCuq92477	Infra bundle upgrades from Cisco UCS Manager release 2.2(3a) fail if performed from Cisco UCS Central when upgrade process becomes unresponsive during 'PollActivateOfUCSM' stage if Cisco UCS Manager does not already contain the management image.	Manually download the Cisco UCS management image or the complete infra bundle to Cisco UCS Manager before triggering the infra upgrade from Cisco UCS Central.	2.2(3a)A Resolved in 2.2(3b)A.
CSCut61527	The Cisco B200M4 blade server reboots unexpectedly when BMC returns invalid FRU information.	This issue does not have a workaround.	Resolved in 2.2(3g)A
CSCur96296	FEX goes online and offline in quick succession under scaled setups.	Avoid IOM/FEX to come back online quickly after it goes offline.	Resolved in 2.2(3g)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuv53399	After IOM firmware upgrade, or after an IOM reset while running effected firmware, Cisco UCS Manager will no longer show Major fault F0481 indicating the IOM encountered a POST failure.	If this issue is encountered, upgrade to a resolved firmware version.	Resolved in 2.2(3k)A
CSCur01379	Cisco UCS fabric interconnects (FI) include a version of bash that is affected by vulnerabilities through CGI scripts and CLI commands while authentication is not required for unauthorized users.	Protect the domain and restrict the access to the management IP address of FIs to block potential exploitation of the vulnerability.	2.0(1q)A Resolved in 2.2(1f)A,2.2(2e)A, 2.2(3b)A
CSCut46044	Cisco Unified Computing Server Management Software (UCSM) includes a version of OpenSSL that is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) IDs: • CVE-2015-0286 • CVE-2015-0287 • CVE-2015-0289 • CVE-2015-0292 • CVE-2015-0293 • CVE-2015-0209 • CVE-2015-0288	This issue has no known workaround	2.2(3a)A Resolved in 3.1(1e)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCup58725	Cisco Unified Computing Server Management Software (UCSM) includes a version of SBLIM-SFCB that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs: • CVE-2010-2054 • CVE-2010-1937	This issue has no known workaround	2.2(3a)A Resolved in 3.1(1e)A
CSCva43666	When the chassis IOM is reset, one of the connected FI server ports gets into the Error disable state at sometimes and all the servers associated with that port are not accessible.	Use the FI port channel or flap the FI fabric port which is in Error disable state.	2.2(3a)A Resolved in 2.2(4b)A
CSCuz20650	When syslog messages are generated continuously, the syslog suspend timer does not recover. Thus, no events are sent to the remote syslog server.	There is no known workaround.	2.2(3a)A Resolved in 2.2(3k)A, 2.2(6i)A, 2.2(7d)A
CSCuu40291	When debug logging is enabled, Cisco UCS Manager tech-support shows that syslogd_debug files are present, but the show debug logfile syslogd_debugs CLI command fails with the following error: `Logfile(syslogd_debugs) does not exist`	Use Cisco UCS Manager tech-support to get syslogd_debug logs.	2.2(3a)A Resolved in 2.2(3k)A, 2.2(6i)A, 2.2(7d)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCux45723	UCS SNMP memory leaks occur when polling FC interfaces and SNMP processes (Walk/Get/Get Bulk) that parse any of the following SNMP MIBs: • fcIfNonLipF8Out • fcIfTimeOutDiscards • fcIfOutDiscards • fcIfCreditLoss • fcIfTxWtAvgBBCreditTransitionToZero	If SNMP memory leaks occur, avoid polling the SNMP MIBs on FC interfaces.	2.2(3a)A Resolved in 2.2(3k)A, 2.2(6i)A

Open Caveats in Release 2.2(2e)

Open Caveats in Release 2.2(2e)

Table 72: Open Caveats in Release 2.2(2e)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCur19358	The firmware upgrade of Nvidia GPUs fails with the error message "FI unreachable". This happens only when Broadcom adapters are used and its firmware is updated along with the firmware of Nvidia GPUs.	Upgrade the firmware for Broadcom adapters first. After the firmware update FSM is complete, another update FSM is triggered with the HFP meant for Nvidia GPU cards.	2.2(2e)A

Open Caveats in Release 2.2(2d)

Open Caveats in Release 2.2(2d)

Table 73: Open Caveats in Release 2.2(2d)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCur21496	Even after the firmware update of the K2 Nvidia GPU adapter is successful, it does not display the version correctly. It displays the older version instead of new version.	This is a cosmetic issue and does not impact the functionality of the GPU cards.	2.2(2d)A Resolved in 2.2(3g)A
CSCup00833	In rare cases, B440 M1 and M2 servers may fail discovery after CIMC activation during upgrade from release 2.0(2q).	In Cisco UCS Manager CLI, use reset slot x/y where x/y designates the B-series server.	2.1(3c)B
CSCup05598	SNMP Community string shows blank text field even after adding and saving the string.	This issue has no known workaround. This is a different convention than previously used but running a simple snmpget or snmpwalk against Cisco UCS Manager VIP with the string just saved should confirm that SNMP is functional. **Note** Although the field is blank, the display of the 'Set: yes' or 'Set: No' notifier indicates the value is present.	2.2(1d)A
CSCup20961	Unable to add VIFs to a service profile or make modifications that require a new VIF on an existing interface, such as when adding fabric failover.	Restart `svc_sam_dme` process.	2.2(1d)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCup38317	In some rare instances, typically during host power on, a board fails to discover and one of the following errors is displayed: `Reason: CIMC did not detect storage controller or CIMC storage subsystem not yet initialized.`	Decommission and reacknowledge the server.	2.2(2c)B
CSCup40056	In some rare cases, if hypervisor and VM storage traffic are sharing the same fNIC(s) and FI is in switching mode and configured with Cisco VIC 1240 and with NPIV on Windows 2012R2, live migrations may fail.	Assign separate fNICs for hypervisor and VM storage traffic. **Note** For more information, refer to troubleshooting technote #117929.	2.2(1d)B

Defect ID	Symptom	Workaround	First Bundle Affected

CSCup40441	In some cases, attempts to remove a service profile that contains two vNICs and two vHBAs from a B200 M3 server with a 61xx FI and a M73KR-Q adapter running release 2.1(3b) will fail with the following error:
	`Unconfigure server from service profile pre-boot environment (sam:dme:ComputePhysicalDisassociate:PnuOSUnconfig)`
	`Error 4106 - Unable to find FC Device.`
	and Discovery fails with this error:
	`Discovery Fail Error: Unable to get Fibre Channel Device Information from the system (sam:dme:ComputeBladeDiscover:PnuOSInventory)`
		This issue is caused by an unsupported WWPN in the service profile. If WWPN has the multicast bit set (Ex.20:01:01:01:31:00:00:23), then Qlogic flags the WWPN as invalid.
		To avoid this issue, always use WWPN with multicast bit turned off
		(Ex. 20:01:00:01:31:00:00:23/20:01: 00:00:31:00:00:23).
		Note This issue can also be avoided by creating WWPN pool from Cisco UCS Manager WWPN template.
		Once the problem occurs, the solution requires an RMA for the card.
			2.1(3b)B

CSCup45930	When upgrading Cisco UCS B230 M2 server from release 2.2(1x) to 2.2(2x) or from 2.2(2x) to 2.2(3x), or when upgrading Cisco UCS C460 M4 server from release 2.2(2x) to 2.2(3x), association fails with “Unable to find storage controller” error.	Reacknowledge the server.	2.2(1e)A Resolved in 2.2(2e)A, 2.2(3c)A
CSCup88161	In certain race conditions when running 2.2(1d) or later firmware, if a memory location which was freed is being used, the 6248 FI kernel crashes with no core.	This issue has no known workaround. If this condition occurs, the system will auto-reboot to a stable condition.	2.1(1d)A Resolved in 2.2(4b)A,

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuq14172	Windows 2012 and Windows 2012R2 systems hang (boot and installation) when TXT is enabled via BIOS setup.	This issue has no known workaround. Disable TXT and reboot.	2.2(2a)B
CSCuq22707	In some cases, vMotion of multiple VMs at the same time causes stale MAC addresses after VM migration, which results in traffic loss between blades attached to the same FI.	This issue has no known workaround. The stale MAC addresses will eventually age out.	2.2(2c)A

CSCuq46105	In some rare cases, the Cisco UCS 6248 FI will unexpectedly reboot with following FI OBFL log in show tech:
	`Uptime: 10964, 0 days 3 hour(s) 2 minute(s) 44 second(s)`
	`Reset Reason: Unknown (0)`
	`Reset Reason SW: Unknown (0)`
	`Reset Reason (HW): uC reset code: 0x0100 ADM1066 Power Good Triggered Reset`
	`Card Mode.........................: Runtime`
		This issue has no known workaround.	2.2(1c)A
			Resolved in 2.2(3c)A.

Defect ID	Symptom	Workaround	First Bundle Affected

CSCuq53385	In some cases, when attempting to regenerate expired self-signed Cisco UCS Manager certificate, Cisco UCS Manager will return the following regarding regeneration of default Key Ring:
	`Cannot Create Certificate Request for default KeyRing`
	`This is accompanied by the following error messages in svc_sam_dme log file in Cisco UCS Manager techsupport log bundle:`
	`=========`
	`[INFO][0xac56abb0][Aug 6 05:20:47.182] [exception_handling:rep] FATAL[5|702]: .. /feature/nuova/sam/sam/src/app/sam/dme/imp/pki/MuPkiEpEndExplicitUpdateCbImp.cc(279): validateKeyRingNodes pkiKeyRing[sys/pki-ext/keyring-default]`
	`: Cannot Create Certificate Request for default KeyRing [INFO][0xac56abb0][Aug 6 05:20:47.183] [exception_handling:rep] ERROR[3|702] .. /feature/nuova/sam/sam/src/lib/framework/core/proc/Doer.cc(874):exceptionCB:`
	`exception encountered during processing: Cannot Create Certificate Request for default KeyRing [702] Cannot Create Certificate Request for default KeyRing`
	`=========`
		To work around this issue, try the following:
		1. When possible, use third-party CA signed keyring from internal or external CA; or
		2. Contact TAC to resolve the error and to regenerate self-signed certificate.
		Note Cisco UCS Manager does not support creating cert-req for default key ring.
			2.1(3d)A

Open Caveats in Release 2.2(2c)

Open Caveats in Release 2.2(2c)

Table 74: Open Caveats in Release 2.2(2c)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuq77241	Inventory scanning software such as Snow Inventory on Windows OS, CIMC, host OS or a remote KVM session may go into unresponsive state.	If the connection to CIMC is alive, resetting the blade power will recover it. If the CIMC is in an unresponsive state or reseting blade power doesn't resolve the issue, resetting the slot will help recover the blade.	2.2(2c)B Resolved in 2.2(6c)B
CSCuz53730	UCSM httpd process may experience high memory usage or crash with a core file showing indications of memory allocation failure.	There is no known workaround.	2.2(2c)A Resolved in 2.2(8f)A
CSCuw02439	When using Cisco UCS M81KR VIC adapters on a system running Cisco UCS Manager Release 2.2(2c), the adapters crash and generate core files. VIC adapter log files display the following error before the adapter crashes: `ecpumgr.main ERROR: ecpu 1 panic: ASSERT FAILED (Exception 2 triggered!) @ mips/ecpu_panic.c:138`	This issue has no known workaround.	2.2(2c)B Resolved 2.2(3k)A, 2.2(6i)B
CSCux59298	When using UCS B200 M3 servers with VIC 1240 on a system running Cisco UCSM Release 2.2(2c), network and SAN lose connectivity.	When this issue occurs, reboot the server.	2.2(2c)B Resolved 2.2(3k)A, 2.2(6i)B

Defect ID	Symptom	Workaround	First Bundle Affected

CSCus32933	Cisco UCS Manager does not display an error message when a WILL_BOOT_FAULT event is raised because of an incorrect CPLD version.	- Issue the following commands;
		`# scope server x/x`
		`# scope boardcontroller`
		`# activate firmware 13.0 force`
		`# commit-buffer`
		- Reset CIMC.
		You might see the following messages in a var/log/messages file in CIMC show tech.
		`:will_boot:3438: platforms/castlerock/check.c:89:Proccessor[0]: Type: 1, Version: 17-10291-09_R01`
		`:will_boot:3438: platforms/castlerock/check.c:97:Ivy Bridge Processor requires update`
		`:will_boot:3438: platforms/castlerock/check.c:89:Proccessor[1]: Type: 1, Version: 17-10291-09_R01`
		`:will_boot:3438: platforms/castlerock/check.c:97:Ivy Bridge Processor requires update`
			2.2(2c)B
			Resolved 2.2(3j)B

Defect ID	Symptom	Workaround	First Bundle Affected
CSCur66094	You may see the following symptoms: • Multiple components stuck in discovery or upgrade state with no FSM progression. • Control plane service issue triggering faults in UCSM. However, the OS on the server works normally. • There may be UCSM process crashes and retries for DME and other processes, but these are not always present.	Contact Cisco TAC to manually restart the bladeAG process as needed on both Fabric Interconnects.	2.2(2c)A Resolved in 2.2(3g)
CSCur05013	Messages.log file on a Cisco UCS B200 M2 blade fails when the log file fills with messages including: `364:BMC lost control of the bus.[0xd 0x0].`	This issue has no known workaround.	2.2(2c)B Resolved in 2.2(3d)B.
CSCur38408	When a PCIe card is present in slot 2 and riser 2 is missing, fabric interconnect HA failover can cause the attached Cisco UCS C460 M4 servers to reboot.	To work around this issue, try one of the following: Move the card in slot 2 to a different slot. Add PCIe riser 2.	2.2(2c)A Resolved in 2.2(3d)A.
CSCuj09403	When installing RHEL 6.3 in UEFI mode with M73KR-Q or M73KR-E adapters, the system hangs with a ‘cannot exit boot services’ message.	This issue has no known workaround with M73KR-Q or M73KR-E adapters. Use VIC1240 adapter or use legacy boot.	2.2(1b)B

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuj63232	In some instances, most commonly after doing a CIMC upgrade, certain long running operation data may indicate that an operation is currently running when it isn't. For example, the consistency check operation may report 0% progress and be stuck in that status.	This issue has no known workaround. To verify that the data is erroneous, use an LSI tool, such as WebBios or MegaCli, to confirm the operation is still in progress.	2.2(1b)A
CSCul85363	Redhat 6.x installation fails on a B200 M3 that uses a Seagate ST300MM0006 single drive JBOD configuration with the No RAID policy.	To work around this issue: Install the OS using custom layout by selecting Create custom layout" when prompted for installation type. Create custom layout and swap partition.	2.2(1b)A
CSCum91845	Server reboots on changing any management policy when Service Profile is derived from update Service Profile Template that has no vNICs.	This issue has no known workaround.	2.2(2c)A
CSCun16169	Ethernet uplink port channel member interfaces are permanently down on primary FI after 20 iterations of port channel flap from Cisco UCS Manager.	Remove and add port channel.	2.2(2c)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCun22459	In some cases when the port is in trunk mode containing more than one isolated-primary VLAN pair, the VM comes up with vNIC configured with two isolated-primary pairs and does not get dynamic IP address.	Use one of the following two options to resolve this issue: **1.** Do not put the port in trunk mode and configure one isolated-primary VLAN pair per port. **2.** Do not set the native VLAN and, instead, explicitly tag the traffic with one of the VLANs.	2.2(2c)A
CSCun29274	In rare cases and only if blade is already discovered with a network adapter and user replaces it with storage adapter, the association or disassociation of that blade server may fail with error reported as "Invalid adapter connectivity, no adapter found."	Decommission and recommission the affected blade.	2.2(2c)A
CSCun79973	In some conditions, when a Cisco UCS Manager user changes the QoS policy on a vNIC where Netflow session is actively enabled on a vNIC with transmit monitoring, the vNIC will hang.	To workaround this issue: **1.** Disable the Netflow session on the vNIC. **2.** Change the QoS policy. **3.** Reenable the Netflow session.	2.2(2c)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCun82594	DIMMS are mapped out during MRC (BIOS POST) when lockstep or mirroring are enabled in configurations with Ivy Bridge or Sandy Bridge CPU and with the following DIMM configurations: • 1866 Hynix - Lockstep/Mirroring - 3 DIMMs Per Channel. • 1866 Samsung - Lockstep/Mirroring - 3 DIMMs Per Channel.	The fix is provided via the Intel Memory Reference Code update.	2.2(2c)B
CSCuo12665	In some cases, when user sets SAN boot for boot policy in service profile, the configured boot policy is not reflected on a blade equipped with a M71KR-Q adapter after association so the blade will not boot from SAN.	One of the following workarounds may resolve this issue: **1.** Reset the blade **2.** Upgrade the server firmware version to match with infra bundle version (FIs / IOMs / Cisco UCS Manager)	2.2(1d)A 2.1(3b)B

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuo34760	In some rare cases, if primary FI gets rebooted and comes back up as subordinate FI, some vEthernet interfaces will remain in down state on the newly subordinate FI (while previous subordinate FI becomes primary).	One of the following workarounds will recover the affected servers: **1.** (Preferred) CIMC reset of affected servers will force shallow discovery of the server which fixes this issue. This will not reboot the server. **2.** IOM reset (which is connected to the affected FI) will also fix this issue. However, traffic going through that IOM for all blade servers on that chassis will be impacted unless there is failover adapter configs supported to redirect traffic through other working IOM/FI. **3.** Reacknowledge affected servers. However, server gets rebooted.	2.1(2d)A
CSCuo38990	In some rare conditions, servers lose network connectivity during failover.	Reboot subordinate FI to recover.	2.1(3b)A
CSCuo41491	If boot policy has PXE boot listed prior to local disk / HBA, a blade my sometimes boot to pnuos instead of following normal boot policy when rebooted.	Re-associate Service Profile.	2.2(1b)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuo51708	In some cases when attempting downgrade in middle of autoinstall upgrade, Cisco UCS Manager autoinstall downgrade will fail.	Manually activate UCSM version to the higher revision, and then let auto-install downgrade it.	2.2(1d)A Resolved in 2.2(1g)A.
CSCuo55182	IPMITool version 14 or 14rc2 cannot obtain any IPMI information on the slave blade in a B460-M4 configuration four-socket configuration.	Use ipmitool version 13.	2.2(2c)B
CSCuo65728	In some instances, a MAC move is not learned by the Cisco UCS FI after a VM is vMotioned between blades when the Cisco UCS FI is enabled with vNIC Fabric Failover and hypervisor is configured to utilize active/standby for vNICs. **Note** This is not a Cisco UCS best practices configuration.	Reset the vEthernet interface on the target vMotion host to force a MAC relearn.	2.2(1c)A
CSCuo87059	In rare cases, backplane ports on an IOM that is providing a NULL serial number to Cisco UCS Manager may be missing after chassis decommission and recommission.	Perform an additional decommission and recommission cycle.	2.2(2c)B Resolved in 2.2(3a)B

Defect ID	Symptom	Workaround	First Bundle Affected

CSCuo98011	Cisco UCS Manager can crash (dump core) during Infra firmware upgrade (ucs-k9-bundle-infra.2.2.2c.A.bin) when upgrade is initiated from Cisco UCS Central if Cisco UCS Manager is registered to Cisco UCS Central using IPv4 address and image bundles are not present in Cisco UCS Manager.
	Note The core dump is associated with the svc_sam_dcosAG process and that process does restart itself after the crash.
		Avoid this issue by using either of two workarounds:
		1. Download the Cisco UCS Manager 2.2(2c) Infra bundle (ucs-k9-bundle-infra.2.2.2c.A.bin) directly on to Cisco UCS Manager before initiating the firmware upgrade from Cisco UCS Central.
		2. Download the firmware image into Cisco UCS Manager and initiate the upgrade directly from Cisco UCS Manager after using the following commands to ensure policy control resolution is set to Local
		CLI in UCSM
		`>scope system`
		`>scope control-ep policy`
		`>set infra-pack-ctrl source local`
		GUI in UCSM
		Go to **Admin** > **UCS Central** > **Policy Resolution Control (Right Pane)**
			2.2(2c)A
			Resolved in 2.2(2d)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuo68579	In some cases after a firmware upgrade, FC traffic stops working on fabric interconnect. However, blades in those chassis have successful flogi into the fabric. On the upstream fabric switch fc4 feature types are missing when checking show fcns database detail for the affected blades.	Reboot affected Fabric Interconnect	2.1(3b)A
CSCuo81734	In some cases, FNIC driver bundled with driver disk does not load when installing on a standalone C-series server and does not return error to indicate failure.	Perform RPM installation after system is up using the inbox FNIC driver.	2.2(1b)A
CSCup07488	ECC sensors report invalid “Upper Non-Recoverable” data when there are existing failed PECI transactions on a blade.	Restart the ipmi stack while the host is up and running and BIOS_POST_COMPLETE is asserted. However, if PECI failures persist on the blade, this task will need to be repeated.	2.2(2c)B Resolved in 2.2(2d)B
CSCut03086	When you auto install infrastructure firmware bundle and UCS Manager FI upgrades, in a VM-FEX scale set up with over 100 servers, DME core will happen.	Restart the DME by doing one of the following: **1.** Start and stop the PMON process. **2.** Kill the PMON process.	Resolved in 2.2(1h)A

Open Caveats in Release 2.2(2a)

Open Caveats in Release 2.2(2a)

Table 75: Open Caveats in Release 2.2(2a)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvh22485	After vMotion/VM migration, VMs are unable to receive broadcast/multicast packets including ARP packets. This happens because the adapter is not removing the VLAN tags from the packets due to incorrect configuration received from the FI. This issue occurs under the following setup: • ESIi or RHEV or CentOS with Ovrit • VMFEX with PVLAN host configurations on the Veths	• Don not perform vMotion/VM migration. If required, power-off and migrate the VM and then power-on. • If this issue has already occurred, If the issue happens, power cycle the VM after vMotion.	2.2(2a)A Resolved in 2.2(8j).
CSCuq63868	When creating a vNIC in a LAN connectivity policy, the show configuration command generates a software error.	No known workaround.	
CSCur16493	Customers with the UCSC-GPU-VGXK2 GPU adapter should update to release 2.2(3f) to receive updated firmware.	Upgrade to release 2.2(2e) and verify that the UCSC-GPU-VGXK2 firmware has been updated to version 80.04.F5.00.03_2055.0552.01.08.	2.2(2a)B Resolved in 2.2(2e)B.

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuo89748	Under rare conditions in a scale deployment, the Cisco UCS Manager GUI may crash with the following error message: `Fatal Error: Event sequencing is skewed, Would you like to login again or exit?`	When this issue occurs, exit the GUI and log in to it again. You may continue to see the error message until the underlying triggering condition is resolved.	2.2(2a)A

Open Caveats in Release 2.2(1f)

Open Caveats in Release 2.2(1f)

Table 76: Open Caveats in Release 2.2(1f)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCur37260	FI upgrade or downgrade may fail due to lack of disk space in /mnt/pss. The following error may be seen: `PL20-B %SYSMGR-2-NON_VOLATILE_DB_FULL: System non-volatile storage usage is unexpectedly high at 99%`	Contact Cisco TAC to recover from this issue.	2.1(3c)A Resolved in 2.2(3d)A.

Open Caveats in Release 2.2(1e)

Open Caveats in Release 2.2(1e)

Table 77: Open Caveats in Release 2.2(1e)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuo97907	Blades using a BIOS policy that utilizes the core multi- processing option do not honor changes made to the policy.	Disable the cores using the operating system.	2.1(3b)A

Open Caveats in Release 2.2(1d)

Open Caveats in Release 2.2(1d)

Table 78: Open Caveats in Release 2.2(1d)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCus03683	The Cisco UCS 6200 series primary and subordinate FIs may reboot unexpectedly due to high volume traffic impacting the management interface.	When this issue occurs, do one of the following: • Apply rate limiting or other QOS policies upstream to prevent large amounts of traffic from hitting the mgmt interfaces of the fabric interconnects. • Apply ACL on upstream devices to only allow connectivity to mgmt interfaces from approved or identified bastion hosts.	2.2(1d)A Resolved in 2.2(4b)A, 2.2(5a)A

Defect ID	Symptom	Workaround	First Bundle Affected

CSCuw36128		When this issue occurs, restart UCSM processes through the CLI:
		`UCS-A# connect local-mgmt`
		`UCS-A(local-mgmt)# pmon stop`
		`UCS-A(local-mgmt)# pmon start`
			2.2(1d)A
			Resolved in 2.2(3k)A, 2.2(6i)A, 2.2(7b)A

Defect ID	Symptom	Workaround	First Bundle Affected
	Under rare conditions, there may be statsAG mts q leaks, and the following fault may be raised: Major Fault F0885: Fabric Interconnect B inventory is not complete card-inventory,eth-pc-inventory,eth-port-inventory,fc-pc-inventory,fc-port-inventory,mgmt-port-inventory,remote-eth-port-inventory,switch-fru seen. (It could be for either A or B side, or even both) The error messages shown in the statsAG log file may include the following: [MAJOR][0x7544eb90][date][app_sam_statsAG:pollF] Error getting switch FRU inventory; details: SC_Send_tlv(3640) cmd_ucsm_req_send_recv() failed(-1) [MAJOR][0x7544eb90][date][app_sam_statsAG:getSw] Error getting Line-Card inventory; details: Internal Error: SC_Execute_show_command() returned -1 [MAJOR][0x7544eb90][date][app_sam_statsAG:getPh] Error getting physical Ethernet port inventory; details: Error in pm_get_if_index_listing(), errno: 16 [MAJOR][0x7544eb90][date][app_sam_statsAG:getRe] Error getting remote physical Ethernet port inventory; details: Error in pm_get_if_index_listing(),		

Defect ID	Symptom	Workaround	First Bundle Affected

	`errno: 16`
	`[MAJOR][0x7544eb90][ date][app_sam_statsAG:getPh]`
	`Error getting physical FC port inventory; details: Error in pm_get_if_index_listing(),`
	`errno: 16`		

CSCut28278	After upgrading the infrastructure and the Cisco UCS Manager image, the subordinate fabric interconnect fails the pre-upgrade check because of insufficient free space in the /var/sysmgr directory.	Contact TAC to verify whether discovery related log files filled the /var/sysmgr directory.	2.2(1d)A Resolved in 2.2(3j)A
CSCur01185	The HA policy of Reset triggers the Cisco UCS 6296UP fabric interconnect to reset.	Check whether NPM is leaking memory by running the `show npv internal mem-stats detail` command on the fabric interconnect To determine which adapter is causing the issue, view the output using the `show npv internal errors` command. The error message will list the VFC causing the issue.	2.2(1d)A Resolved in 2.2(3j)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCup95855	Cisco UCS C240 M3 server upgrades fail because FSM tasks are stuck in the throttled state in Cisco UCS Manager.	-Verify that all CIMCs are accessible from the UCSM CLI (connect cimc X/Y for blades and connect cimc X for racks) -Resolve all communication issues between UCSM and any inaccessible CIMC. -Verify that netstat -anop output does not show receive queues filling up -Before running the restart dme command to recover from this scenario, take a core dump of the dme to analyze this situation further. Use the kill -s SIGABRT <dme pid> command to generate the core of the svc_sam_dme_process. -Copy the generated core and attach it to SR or the bug for further analysis	2.2(1d)A Resolved in 2.2(3j)A, 2.2(6c)A
CSCuu15250	Toggling the Fabric Interconnect (FI) locator LED in UCSM fails with the following symptoms: • UCSM GUI—The Locator LED will continue spinning and the On/Off options will be grayed out. • UCSM CLI—The following error will appear: `Error: Managed object doesn't exist`	When this occurs, contact TAC to toggle the FI locator LED by using the debug plug-in access to NXOS.	2.2(1d)A Resolved in 2.2(5c)A.

Defect ID	Symptom	Workaround	First Bundle Affected
CSCus64439	Cisco UCS Manager Mezz logs and VMware vmkernel logs indicate storage latency and numerous FNIC aborts.	Reboot blade servers where the PGS and PFC features are not in the right order. To avoid this issue, first upgrade any Cisco UCS 1240, Cisco UCS 1280, and Cisco M81KR adapter firmware before updating the Cisco UCS infrastructure components—Cisco UCS Manager, IOM, and FI.	2.2(1d)B resolved in 2.2(3h)B
CSCus11782	After rebooting a Cisco UCS 6248UP Fabric Interconnect (FI) that is operating in the FC end-host mode, some member links of the SAN port channel do not come up. Running the show interface brief command on the FI displays the notConnected status. On the Cisco Nexus switch, the corresponding ports show as invalidCfg.	When this issue occurs, do one of the following: • Run the shut and no shut commands on the non-working interfaces of the Cisco Nexus switch. • Enable trunking on the Cisco UCS Fabric Interconnect and Cisco Nexus switch.	2.2(1d)A Resolved in 2.2(5b)A, 2.2(3j)A
CSCus12019	MAC address table on the FI not updated immediately after a MAC move or change.	There are two possible workarounds: • The MAC address is updated automatically after a while (could range from a few seconds to a few minutes). • The MAC address update can be forced by clearing the MAC address table manually by using the clear mac address-table dynamic command.	2.2(1d)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuo11700	In rare cases, a context switch while applying a new sam.config triggers a race condition that causes the httpd.sh or ucssh process to crash.	The httpd.sh process will recover after the crash. To fix the ucssh process crash, re-launch the Cisco UCS Manager CLI.	2.2(1d)A
CSCuo60330	After upgrading the fabric interconnect to release 2.2(2) or later, the IOMs are unreachable, HA is not ready, and previous server interfaces show no configuration.	Contact Cisco TAC to recover from this issue.	2.2(1d)A
CSCul44421	You may see the "error accessing shared-storage" fault in Cisco UCS Manager. This message may appear any time but is seen more often during an FI reboot, upgrade, or IOM reset when running release 2.x of Cisco UCS Manager.	This issue has no known workaround. This fault is auto-cleared and transient so should not persist. The HA framework remains INTACT as long as show cluster extended output reports state as PRIMARY_OK.	2.1(2d)A Resolved in 2.2(1e)A and 2.2(2c)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCum98771	Upgrading from Cisco UCS Manager 2.1(2a) or higher to release 2.2(1x) with FlexFlash State enabled in local disk policy of service profiles on servers causes the “FlexFlash controller error, probably not supported, not equipped or inoperable” config-failure. This condition prevents updates to Blade and Rack firmware package bundles using auto-install or host firmware pack.	Avoid this error using either of two workarounds: **1.** Disable FlexFlash in local disk policy of service profile. This will resolve the config-failure and CIMC can be upgraded using auto-install and host firmware pack. Since disabling FlexFlash requires host reboot, host downtime is required. **2.** Modify host firmware pack in service profile to use empty blade and rack package versions. Then directly update and activate CIMC firmware (Equipment > Chassis > Server > Inventory > CIMC).	2.2(1b)A Resolved in 2.2(1e)A and 2.2(2c)A
CSCun25187	When using third-party certificates with Cisco UCS Central, status of Cisco UCS Manager might be displayed in Cisco UCS Central as 'Lost-Visibility' if a keyring with a certificate chain is configured to use https communication. This occurs when certificates are signed by subordinate CA instead of root CA.	Use third-party certificates that are signed directly by root CA for UCS Central https communication.	2.1(2a)A Resolved in 2.2(1e)A and 2.2(2c)A
CSCun86873	In some cases, during initial discovery or following upgrade-initiated discovery, B230 M2 shows only 8 of 10 cores available.	Reacknowledge the blade.	2.2(1c)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuo12230	When vNIC of a service profile is configured to allow a VLAN defined in appliances cloud in the LAN configuration, the show run interface vethernet <x> and show interface vethernet <x> switchport command outputs report different VLANs allowed on the virtual Ethernet interface.	Check the outputs listed in the symptoms to confirm the problem. If the output shows the problem, then move the VLAN from the appliance cloud to the LAN cloud.	2.2(1c)A
CSCus74206	After disconnecting then re-connecting a cable between Fabric Interconnect and IOM, all VFC interfaces on the chassis are flapped once.	Remove the Pin Group setting in vHBA to use Dynamic Pinning instead of Static Pinning.	2.2(1d)A Resolved in 2.2(3g)

Defect ID	Symptom	Workaround	First Bundle Affected

CSCuo78883	‘Application Blocked by Security Settings’ error when starting the Cisco UCS Manager GUI or KVM Console application.
	Because the Java Code Signing Certificate expired, users on Java 7 update 40 or higher might see the following message:
	`Application Blocked by Security Settings.`
	`Your security settings have blocked an application signed with an expired or not-yet-valid certificate from running.`
			2.2(1b)A
			Resolved in 2.2(1e)A and 2.2(2c)A

Defect ID	Symptom	Workaround	First Bundle Affected
		To fix this issue, you can either temporarily lower your Java security settings to add Cisco UCS Manager as an exception or, if you are using Java 7 update 51 or higher, you can add the Cisco UCS Manager host IP address to the Exception Site list. To perform one of these workarounds, perform the corresponding steps below: To temporarily lower your security settings: **1.** Start Java Control Panel. (Location may vary depending on operating system and browser preferences.) **2.** Lower the Security level to Medium. **3.** Start Cisco UCS Manager. **4.** In warning popup, check “I accept the risk and want to run this application” checkbox and click Run. **5.** Return to the Java Control Panel and reset your security level. To add the IP address to the exception site list (for Java 7 version 51 and higher): **1.** Start Java Control Panel. (Location may vary depending on operating system and browser preferences.)	

Defect ID	Symptom	Workaround	First Bundle Affected
		2. In Security area, click Edit Site button to add IP address to the list. **Note** If you use HTTPS to access Cisco UCS Manager, ensure that you have the correct prefix. 3. Click OK.	
CSCup61601	FCOE_MGR crashes if FI is configured with too many noncontiguous VLANs.	Decrease the number of noncontiguous VLANs on the FI.	2.2(1d)A Resolved in 2.2(2d)A
CSCup61947	In some cases, MAC learning fails after adding 1000 or more VLANs with a large PV count with 120 or more virtual interfaces each with 1000 VLANs.	To account for this issue, monitor the `dleft_lif_vlan_mbr` table to ensure total VLANs does not exceed 16,000. If VLAN total approaches or exceeds this limit, reduce VLAN count and then reboot the FI as needed to recover from a MAC learning failure state.	2.2(1d)A Resolved in 2.2(2d)A
CSCup82677	A Cisco UCS system with ESXi OS will not exceed 10Gb speed even when QoS is configured with line-rate of 20Gb or 40Gb.	To resolve this issue, set the Rate(Kbps) value in the QoS policy to be the desired value above 10000000. The value must be numeric, such as 20000000 or 40000000.	2.2(1d)A Resolved in 2.2(2d)A
CSCus85186	After activating Cisco Trusted Platform Module (TPM), the enable and active statuses remain as disabled and deactivated.	This issue has no known workaround.	2.2(1d)B Resolved in 2.2(1h)B, 2.2(3j)B, 2.2(4b)B

Defect ID	Symptom	Workaround	First Bundle Affected
CSCut09151, CSCut21914 and CSCut08605	System Management BUS (SMBUS) traffic will collide on the SMBUS shared by the host and CIMC. As a result, certain system failures such as false thermal alarms may happen.	Avoid running OS applications that access the host SMBUS.	Resolved in 2.2(1h)A
CSCuo50049	Cisco UCS Manager will experience HA cluster failover after upgrading from Release 1.4.	This issue has no known workaround.	Resolved in 2.2(1h)A

Open Caveats in Release 2.2(1c)

Open Caveats in Release 2.2(1c)

Table 79: Open Caveats in Release 2.2(1c)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCum82888	After upgrading to Release 2.2(1b), you may see the following errors: • No access to the Cisco UCS Manager GUI. • The virtual IP is not reachable. • The virtual IP cannot be accessed by the GUI or CLI/SSH. • Individual FIs can be accessed using SSH but not with http. This occurs when the default keyring is deleted before upgrade, or if the default keyring is deleted after the upgrade and the system is rebooted.	To avoid this issue, do not delete the default keyring. If this issue occurs, stop the bladeAG process.	2.2(1b)B Resolved in 2.2(1d)B

Defect ID	Symptom	Workaround	First Bundle Affected
CSCum09954	If an FC uplink interface is set to administratively shut, after upgrading to Release 2.2(1b) you may see a "FCoE or FC uplink is down on Vsan 202" error.	This issue is cosmetic and the error message can be safely ignored.	2.2(1b)A Resolved in 2.2(1d)A
CSCum60793	You may see the following fault in Cisco UCS Manager: `[FSM:STAGE:RETRY:]: Report mount suspend success to operations manager errors` This occurs if Cisco UCS Central is not reachable or the domain has been unregistered.	Restore connectivity to Cisco UCS Central, or register the domain again.	2.1(2c)A
CSCuo79500	Service dcosag falsely displays information that indicates a vNIC with a usNIC connection policy was automatically changed to dynamic vNIC when a customer adds a second vNIC with a usNIC policy.	This issue does not effect functionality. The usNIC policies are properly set; the radio button selection falsely displays the selection of dynamic vNIC policy. Saved changes can be seen by clicking on the usNIC radio button.	2.2(1c)A Resolved in 2.2(2d)A
CSCut54264	CIMC internal linux iptables deny additional mcserver connections between the CIMC and Fabric Interconnect.	Reset CIMC of the impacted servers.	2.2(1c)A Resolved in 2.2(3g)B

Open Caveats in Release 2.2(1b)

Open Caveats in Release 2.2(1b)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvm02934	Cisco UCS B-Series M2 servers and 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.	The fix for CVE-2018-3620 (OS/SMM) and CVE-2018-3646 (VMM) requires applying the updated processor microcode from Intel® as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. For more information, please see the Cisco Security Advisory available here: CPU Side-Channel Information Disclosure Vulnerabilities: August 2018	3.2(1d)B, 3.2(1d)C 3.1(1e)B, 3.1(1e)C 2.2(1b)B, 2.2(1b)C CSCvm02934 is resolved in 2.2(8l)B, 2.2(8l)C

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvm03356	Cisco UCS B-Series M3 servers and C-Series M3 servers are based on Intel® processors that are vulnerable to exploits that use CPU speculative processing and data cache timing to potentially identify privileged information. These exploits are collectively known as L1 Terminal Fault (L1TF). • CVE-2018-3615 (affecting SGX), also known as Foreshadow, is not known to affect any existing Cisco UCS servers because Cisco UCS M5 and earlier generation servers, and HyperFlex M5 and earlier generation servers do not use Intel® SGX technology. • CVE-2018-3620 (affecting OS/System Management Mode) and CVE-2018-3646 (affecting Virtual Machine Monitors) are referred to as L1 Terminal Fault attacks by Intel®. These vulnerabilities are mitigated by applying the updated processor microcode from Intel included in the server firmware bundle, and the relevant Operating System and Hypervisor patches from the appropriate vendors.	The fix for CVE-2018-3620 (OS/SMM) and CVE-2018-3646 (VMM) requires applying the updated processor microcode from Intel® as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. For more information, please see the Cisco Security Advisory available here: CPU Side-Channel Information Disclosure Vulnerabilities: August 2018	4.0(1a)B, 4.0(1a)C 3.2(1d)B, 3.2(1d)C 3.1(1e)B, 3.1(1e)C 2.2(1b)B, 2.2(1b)C CSCvm03356 is resolved in 2.2(8l)B, 2.2(8l)C

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvm03351	Cisco UCS B-Series M4 servers, C-Series M4 servers, S3260 M4 storage servers, and HyperFlex M4 servers 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.	The fix for CVE-2018-3620 (OS/SMM) and CVE-2018-3646 (VMM) requires applying the updated processor microcode from Intel® as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. For more information, please see the Cisco Security Advisory available here: CPU Side-Channel Information Disclosure Vulnerabilities: August 2018	4.0(1a)B, 4.0(1a)C 3.2(1d)B, 3.2(1d)C 3.1(1e)B, 3.1(1e)C 2.2(1b)B, 2.2(1b)C CSCvm03351 is resolved in 2.2(8l)B, 2.2(8l)C

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvj59299 CSCvj59301	Cisco UCS B-Series and C-Series M2 servers are based on Intel® Xeon® 5500, 5600, and Ex 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 relevant Operating System patches using an interface provided by updated processor microcode included in the server firmware bundle.	The fix for CVE-2018-3639 (Spectre/Variant #4) and CVE-2018-3640 (Spectre/Variant #3a) requires applying the updated microcode from Intel as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. For more information, see the Cisco Software Advisory at https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180521-cpusidechannel	3.1(1e)B, 3.1(1e)C 3.2(1d)B, 3.2(1d)C 2.2(1b)B, 2.2(1b)C
CSCvj54880 CSCvj54847 CSCvj54187	Cisco UCS M3 and M4 servers, and Hyperflex M4 servers are based on Intel® processors that are vulnerable to variants of an exploit that uses CPU speculative processing and data cache timing to efficiently leak information, known as Spectre. CVE-2018-3639 (Spectre/Variant #4) and CVE-2018-3640 (Spectre/Variant #3a) are addressed by relevant Operating System patches using an interface provided by updated processor microcode included in the server firmware bundle.	The fix for CVE-2018-3639 (Spectre/Variant #4) and CVE-2018-3640 (Spectre/Variant #3a) requires applying the updated microcode from Intel as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. For more information, see the Cisco Software Advisory at https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180521-cpusidechannel	3.1(1e)B, 3.1(1e)C 3.2(1d)B, 3.2(1d)C 2.2(1b)B, 2.2(1b)C 3.0(1c)B, 3.0(1c)C - Only for M3, M4 EP
CSCuu83383	UCS Manager includes a version of OpenSSL that is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) IDs: CVE-2015-4000, CVE-2015-1788, CVE-2015-1789, CVE-2015-1790, CVE-2015-1792, CVE-2015-1791, CVE-2014-8176	There is no known workaround.	1.1(1j)A Resolved in 2.2(8i)A
CSCvd02546	During a UCS Manager upgrade from 2.2(3l) to 3.1(2) only the secondary Fabric Interconnect may be upgraded.	There is no known workaround.	2.2(1b)A Resolved in 2.2(8i)A

Defect ID	Symptom	Workaround	First Bundle Affected

CSCuz55693	When you attempt to reset memory errors using the following commands:
	`ucs-fi chassis/server #`
	`reset-all-memory-errors`
	Cisco UCS Manager may generate a 'Managed object does not exist' error.
		The command will work after you perform a de-commission of the new blade and then re-acknowledge it.	2.2(1b)A
			Resolved in 2.2(3l)A

CSCuv20324	The FCoE storage, in rare cases, becomes unavailable or performs very poorly. This can occur after a reset of either host-attached switch in the case of standalone systems, or after the reset of an IOM or FI in UCS-managed systems when the IOM or FI sends configuration information to the adapter later than 5 seconds after link-up.	Reboot the affected host after switch or IOM reset is completed.	2.2(1b)B Resolved in 2.2(6g)B
CSCum50468	After upgrading the UCS Manager to version 2.2(6c) or higher, false faults for Fabric VSAN Membership Down are not clearing.	This issue has no known workaround.	2.2(1b)A
CSCuj63448	When upgrading to a catalog that supports new DIMMs, some of the DIMM information is not displayed.	Reacknowledge the blade server.	1.4(4k)A
CSCui67824	When you disable port security from a network control policy with Hyper-V port profile, security is disabled on the nested port-profile, but security remains enabled on a few interfaces.	This issue has no known workaround.	2.2(1b)A
CSCuj26767	Attempting to install UEFI OS second time sets incorrect boot order and stops installation.	Clean initial installation in the disk and restart installation.	2.2(1b)A
CSCui52680	When the blade appears to be in normal operation state, Cisco UCS Manager SEL message list might display the following error: EFI Load Image Security Violation	If all blade functions appear to be normal, ignore this error message.	2.2(1b)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCud75506	The UUID is translated incorrectly when you upgrade ESXi from version 4.1 or 5.1 on the Cisco UCS B200 M3, B220 M3, or B440 M3 blade servers.	This is a display issue only, and does not affect the service profiles associated with the blades. This issue has no known workaround.	2.0(2r)A
CSCug25894	During Cisco 2100 Series IOM boot and chassis reacknowledgment, sysmgr cores are seen.	The system resumes normal behavior after process restart. This should take approximately three minutes.	2.0(4a)A
CSCul74278	In some cases, if the boot policy is initially configured only for SAN devices and the policy is later modified to add local disk or local HDD device, the server fails to boot from the local disk.	Reacknowledge the server.	2.2(1b)A Resolved in 2.2(2c)A
CSCum02561	When upgrading to 2.2(1b) from 2.1(3a), if you upgrade the infrastructure (A bundle) before the host firmware (B and C bundles), and then modify the service profile you may experience one or more of the following issues: **1.** The configured boot order in the Cisco UCS Manager GUI does not display SAN and local disk. **2.** The server reboots every time the service profile is modified.	**1.** To view missing entries for the configured boot order, use the Cisco UCS Manager CLI to scope into the server and run show boot-order. **2.** To avoid server reboots, uncheck the Reboot on Boot Order Change checkbox before upgrading. **3.** Upgrade the B and C bundles.	2.2(1b)A Resolved in 2.2(1d)A
CSCuj74570	A Cisco UCS B420 M3 blade with a VIC 1240 and a port expander is successfully discovered in a chassis with a 2104XP IOM, even though it is unsupported. When upgrading to the 2204XP IOM, the blade reboots for discovery.	This issue has no known workaround. The B420 M3 blade with port expander is not supported with the 2104XP IOM.	2.1(2a)B

Defect ID	Symptom	Workaround	First Bundle Affected
CSCul72408	During upgrade, the following issues occured: • The IOM backplane ports show admin down in the Cisco UCS Manager GUI. • The VIFs show non-participating. • The adapter shows DCE interfaces down.	Reboot the IOM in the affected chassis.	2.1(3a)A
CSCul95501	IOM FSM failed after downgrading from 2.2(1b). Connectivity between the IOM and the FI could not be established.	Reboot the FI.	2.1(3a)A
CSCuh89441	On B420 M3, the installed OS fails to boot from SAN LUN with Gen-3 E.	Enable EDD 3.0 using the Emulex M73KR-E FCoE option ROM.	2.2(1b)A
CSCuj89557	In some rare conditions, it is observed during Cisco UCS Manager upgrade, downgrade, or FI reload in a cluster setup that Cisco UCS Manager may fail on the secondary FI due to database corruption.	If you detect a db corruption in the secondary FI, erase the database from the FI and reconnect it to the cluster. The secondary syncs up with the primary FI and recreates the db.	2.2(1b)A
CSCtl04654	Changing native VLAN on uplink ports will cause the ports state to change and traffic disruption.	If native VLAN changes are required on uplink ports, we recommend that they be performed during a maintenance window.	2.1(1a)A
CSCuj78615	The EFI Shell boot option is disabled in the BIOS Setup Utility > Boot Options page. Shell Boot option is not automatically launched by the BIOS.	Boot UEFI shell by using either one of the following two options: • Enter BIOS set up utility and select Shell boot option from the Exit and Save page. • Hit F6 to access boot override menu.	2.2(1b)A

Defect ID	Symptom	Workaround	First Bundle Affected

CSCuh13333	When you install ESXi in UEFI mode, the OS fails to boot-up. Even when you seem to have a smooth installation, the server does not boot the ESXi OS.	Do the following:
		1. Boot to Shell.
		2. Determine fsxx (xx is where ESX is installed. It will be typically 0 i.e fs0:) Make sure you have the following:
		`fsxx:\EFI\Boot\BOOTX64.EFI`
		3. Use following command to get current list of EFI Boot Options
		`bcfg boot dump`
		`Note last boot option number to use as LAST_BOOT_No +1`
		4. Use the following command to add new Boot Option at position LAST_BOOT_NO + 1
		`Last parameter in quotes can be any description for new`
		`Boot Option.`
		`This will be displayed during`
		`BIOS F6 menu.`
		`bcfg boot add LAST_BOOT_NO + fsxx:\EFI\BOOT\BOOTX64.EFI UEFI : ESXi`
		5. Make the newBoot Option for ESX as the first by using the following
		`bcfg boot mv LAST_BOOT_NO + 4 1`
		6. Issue reset command at the shell and reset the platform. Press F6 when BIOS is booting to get into BIOS Boot Selection menu. Make sure the new Boot Option is displayed and select this option to Boot ESXi.
			2.2(1b)A

CSCuj31559	Installing Windows EFI PXE using UEFI is slow when compared to the installation using vNIC on MLOM.	This issue has no known workaround.	2.2(1b)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuh34516	Installing Linux PXE using UEFI fails with the following message: `Trying to allocate 971 pages for VMLINUZ.`	This issue has no known workaround.	2.2(1b)A
CSCuj34520	TFM information in UCS Manager inventory contains invalid characters.	This issue has no known workaround.	2.1(2a)A
CSCuj81245	Multiple FNIC aborts in OS kernel and adapter logs when user starts a heavy write operation to SAN disk.	Change IO throttle count from 16 to 256.	2.2(1b)A Resolved in 2.2(2c)B
CSCun25692	Under certain timing conditions while allocating memory to critical data structure, M71KR-Q could run out of heap resulting in SAN boot failure.	To restore expected CNA behavior, downgrade to 2.1(3a) release or upgrade to version where this issue has been resolved.	2.2(1b)B Resolved in 2.2(1e)B and 2.2(2d)B
CSCus42584	The Cisco B200 M4 server unexpectedly reboots after replacing the IOM cables.	This issue does not have a workaround.	Resolved in 2.2(3g)A
CSCut03052	IP QoS core may happen in a VM-FEX scale set up, when you reboot Fabric Interconnects back to back.	Do the following: **1.** Reboot the secondary Fabric Interconnect and wait for discovery/association to stabilize. **2.** Reboot the primary Fabric Interconnect.	Resolved in 2.2(4b)A
CSCut63966	Switch will stop at loader prompt upon reboot due to incorrect boot variables or /opt corruption.	A workaround for this issue is to modify a script file, which is called before any reboots occur. This modification can limit the chances of experiencing this issue during an upgrade to firmware versions in which this issue is resolved. Contact Cisco TAC for more information regarding this workaround, and to recover from this issue.	Resolved in 2.2(1h)A, 2.2(3g)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCus83447	A leap second update causes Cisco UCS Fabric Interconnect to reload or switchover.	Do the following: **1.** Remove NTP configuration from Cisco UCS Manager at least 25 hours before the scheduled leap second. **2.** Restore the previous NTP configuration after the leap second event.	Resolved in 2.2(1h)A, 2.2(3e)A
CScur54705	Cisco UCS Manager sends the UCS Manager username and password hashes to the configured SYSLOG server every 12 hours.	This issue does not have a workaround.	Resolved in 2.2(1h)A
CSCur88952	svc_dam_dme core will happen after upgrading or downgrading to Cisco UCS Manager Release 2.1(b).	This issue does not have a workaround.	Resolved in 2.2(1h)A
CSCva54957	A reboot is triggered without a "user -ack" when modifying a service profile that requires a reboot while shallow association is failing.	This issue does not have a workaround.	2.1(3a)A Resolved in 2.2(8b)A

Open Caveats in Release 2.2(1a)

Open Caveats in Release 2.2(1a)

Table 80: Open Caveats in Release 2.2(1a)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvc48423	Downloading a bundle more than 1GB in size from a local desktop may fail.	Use remote download rather than local download.	2.1(1a)A Resolved in 2.2(8g)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuz91263	A vulnerability in the command-line interface (CLI) of the Cisco Unified Computing System (UCS) Manager and UCS 6200 Series Fabric Interconnects could allow an authenticated, local attacker to access the underlying operating system with the privileges of the root user.	This issue has no known workaround.	2.2(1a)A Resolved in 2.2(8c)A
CSCuz92668	Versions of Network Time Protocol daemon (ntpd) package are affected by one or more vulnerabilities that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or modify the time being advertised by a device acting as a Network Time Protocol (NTP) server. These DoS vulnerabilities and logic issues may allow an attacker to shift a system's time.	This issue has no known workaround.	2.2(1a)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuj84274	When Cisco UCS B-Series servers are configured with the IPMI interface enabled, a vulnerability in the Cisco Integrated Management Controller (CIMC) on the Cisco Unified Computing System Series Platforms may allow an unauthenticated, remote attacker to obtain the password hashes residing on the affected device. The vulnerability is due to the implementation of an insecure authentication protocol. An attacker may exploit this vulnerability by sending a crafted packet to the CIMC of an affected device. An exploit may allow the attacker to receive a response from the CIMC that contains an RKMP message that will allow an attacker to obtain the password hashes for the system, which can then be used in an offline cracking attack.	Disable the IPMI interface on the CIMC running on the UCS system.	2.1(3A) Resolved in 3.1(1e)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCul97240	When a UCS rack server is present in a UCS setup, DHCP renewal occurs frequently and Error level syslog messages are continuously sent to the syslog server configured through Cisco UCS Manager. However, these are false alarms because they do not affect the system. Sample syslog message: `0555 2016 Dec 12 12:07:55 UCS-A-1-A %DAEMON-3-SYSTEM_MSG: uid lease 127.5.99.2 for client 2c:2e:10:10:10:10 is duplicate on 10.1.0.0/10 - dhcpd`	Change the logging level to higher than Error(3). However, this may lead to some critical information not being logged.	2.2(1a)A Resolved in 2.2(7c)A
CSCuv55823	Faults like the following may occur when incompatible combinations of CIMC firmware and UCS Manager firmware are installed at the same time: `Controller 1 on server 1/2 is inoperable: Reason: CIMC did not detect storage controller`	Use the same bundle version of CIMC firmware and UCS Manager firmware.	2.2(1a)A Resolved in 2.2(6e)A
CSCus20526	Adaptor firmware update fails in a high availability UCS set up with a single IOM connected to a FI.	Establish the connectivity between both the IOMs and FIs for UCS high availability.	2.0(1a)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuv49345	When the server is discovered from only one Fabric Interconnect (FI), and the DME primary instance is the other FI, disassociation of the associated service profile fails with the following message: `No connection to MC endpoint` The show fsm state command under server scope will show that the FSM failure is at ResetSecureBootConfiguration	Decommission the server, then recommission it.	2.2(1a) Resolved in 2.2(5c)A
CSCus91342	The blade server needs to reboot after adding a VLAN to a vNIC template.	Reboot the blades for the change to take effect.	Resolved in 2.2(3g)A.
CSCus69458	A heap-based buffer overflow vulnerability in the GNU C library may allow an attacker to obtain sensitive information from an exploited system or, in some instances, perform remote code execution with the privileges of the application being exploited. This vulnerability is documented in Common Vulnerability and Exposures (CVE) CVE-2015-0235.	This issue has no known workaround.	1.0(2k)A Resolved in 2.2(3e)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCur29264	The HTTPS interface of Cisco UCS Manager supports SSLv3 by default, and is vulnerable when using SSLv3 clients to connect. This vulnerability is documented in Common Vulnerability and Exposures (CVE) CVE-2014-3566.	Disable SSLv3 from web clients when connecting to UCSM or when launching KVM using direct access.	2.2(3a)A Resolved in 2.2(3d)A
CSCuj71400	Cisco UCS Manager displays the ’FCoE or FC uplink is down on VSAN X' fault when the member ports for the VSAN are up.	If this error occurs, do the following: **1.** Unconfigure the uplink interface. **2.** Reconfigure it as a FC uplink.	Resolved in 2.2(3k)A, 2.2(6i)A
CSCuo93591	For a fabric interconnect in end-host mode, the MAC address table aging time can get stuck at 300. When this happens, the value cannot be changed through UCSM GUI or CLI.	No known workaround.	Resolved in 2.2(3k)A
CSCux95107	Network Time Protocol configuration on a Cisco UCS blade server includes a version of ntpd package that is affected due to security issues with Network Time Protocol Zero Origin Timestamp Bypass.	This issue has no known workaround.	Resolved in 2.2(7c) A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuz86450	The order property on the adaptorHostIf (adpatorHostEthIf / adaptorHostFcIf) is user-modifiable. The property can be mistakenly set with a value that is different from what it was already set, and can cause the server reboot.	It is strongly recommended that you do not change the order property value because it is internally maintained by Cisco UCS, however for this issue, you can fix the order property to the actual operorder set on the corresponding vnicEther/vnicFc with power tool scripts.	1.4(1j)A Resolved in 2.2(7d)A, 2.2(8b)A
CSCus20526	Adaptor firmware update fails in a high availability UCS set up with a single IOM connected to a FI.	Establish the connectivity between both the IOMs and FIs for UCS high availability.	2.0(1a)A
CSCuv49345	When the server is discovered from only one Fabric Interconnect (FI), and the DME primary instance is the other FI, disassociation of the associated service profile fails with the following message: `No connection to MC endpoint` The **show fsm state** command under server scope will show that the FSM failure is at ResetSecureBootConfiguration	Decommission the server, then recommission it.	2.2(1a) Resolved in 2.2(5c)A
CSCus91342	The blade server needs to reboot after adding a VLAN to a vNIC template.	Reboot the blades for the change to take effect.	Resolved in 2.2(3g)A.

Defect ID	Symptom	Workaround	First Bundle Affected
CSCus69458	A heap-based buffer overflow vulnerability in the GNU C library may allow an attacker to obtain sensitive information from an exploited system or, in some instances, perform remote code execution with the privileges of the application being exploited. This vulnerability is documented in Common Vulnerability and Exposures (CVE) CVE-2015-0235.	This issue has no known workaround.	1.0(2k)A Resolved in 2.2(3e)A
CSCur29264	The HTTPS interface of Cisco UCS Manager supports SSLv3 by default, and is vulnerable when using SSLv3 clients to connect. This vulnerability is documented in Common Vulnerability and Exposures (CVE) CVE-2014-3566.	Disable SSLv3 from web clients when connecting to UCSM or when launching KVM using direct access.	2.2(3a)A Resolved in 2.2(3d)A
CSCuj71400	Cisco UCS Manager displays the 'FCoE or FC uplink is down on VSAN X' fault when the member ports for the VSAN are up.	If this error occurs, do the following: **1.** Unconfigure the uplink interface. **2.** Reconfigure it as a FC uplink.	Resolved in 2.2(3k)A, 2.2(6i)A
CSCuo93591	For a fabric interconnect in end-host mode, the MAC address table aging time can get stuck at 300. When this happens, the value cannot be changed through UCSM GUI or CLI.	No known workaround.	Resolved in 2.2(3k)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCux95107	Network Time Protocol configuration on a Cisco UCS blade server includes a version of ntpd package that is affected due to security issues with Network Time Protocol Zero Origin Timestamp Bypass.	This issue has no known workaround.	Resolved in 2.2(7c) A
CSCuz86450	The order property on the adaptorHostIf (adpatorHostEthIf / adaptorHostFcIf) is user-modifiable. The property can be mistakenly set with a value that is different from what it was already set, and can cause the server reboot.	It is strongly recommended that you do not change the order property value because it is internally maintained by Cisco UCS, however for this issue, you can fix the order property to the actual operorder set on the corresponding vnicEther/vnicFc with power tool scripts.	1.4(1j)A Resolved in 2.2(7d)A, 2.2(8b)A
CSCus20526	Adaptor firmware update fails in a high availability UCS set up with a single IOM connected to a FI.	Establish the connectivity between both the IOMs and FIs for UCS high availability.	2.0(1a)A
CSCux63909	FC abort is observed while running uplink port flap test on uplink Ethernet port-channel from an FI to a Cisco Nexus 7000 switch.	No known workaround.	2.0(2m)B Resolved in 2.2(6j)B, 2.2(7c)B, 2.2(8a)B

Behavior Changes

Release 2.2(8a) introduces the following behavior changes:

- CSCux87408—Initializing the chassis seeprom takes too long to complete.
    - Old behavior: In a new chassis, if the chassis seeprom is not initialized, IOMs are not discovered on certain slots. The chassis seeprom takes too long to initialize. IOM behavior is as follows:
        - A new IOM that has never reached a stable state, and that is running any version of Cisco UCS Manager Release 2.2(6) will be stuck in uboot after 4 attempts of booting each Release 2.2(6) image.
        - An IOM that has previously reached a stable state, and that is running any version of Cisco UCS Manager Release 2.2(6) will go into an infinite reboot loop.

  - New behavior: In a new chassis, if the chassis seeprom is not initialized, IOMs that are running any version of Cisco UCS Manager Release 2.2(x) except Release 2.2(6) can now be discovered on all slots. The chassis seeprom now initializes in the expected time. IOMs running on Release 2.2(6) are discovered if the chassis seeprom is already initialized.
  - Impact: The chassis seeprom now initializes in the expected time.

- CSCtx87011—TPM details are inconsistent in Cisco UCS Manager GUI and CLI.
  - Old behavior: The following TPM details were displayed in the Cisco UCS Manager GUI, but were missing from the output of the **show tpm detail** command—Presence State, and Type.
  - New behavior: The TPM details shown in the output of the **show tpm detail** command and the Cisco UCS Manager GUI are now consistent.
  - Impact: Customers can now list all TPM details through the Cisco UCS Manager CLI as well as the Cisco UCS Manager GUI.

Release 2.2(7b) introduces the following behavior changes:

- CSCtx87011—Cisco UCS backup should preserve identities by default.
  - Old behavior: By default, **Preserve Identities** is not selected in the GUI when the backup operation is initiated.
  - New behavior: By default, **Preserve Identities** is now selected in the GUI when the backup operation is initiated.
  - Impact: With Preserve Identities selected by default, allocated identities such MAC addresses, UUIDs, WWxNs and server assignments will be preserved in the backup file. This will allow the system be restored with the exact same identity assignments. To perform a backup of the logical configuration that can be re-used in other systems, customers must clear this selection when performing the backup operation.

Release 2.2(6c) introduces the following behavior changes:

- CSCuu16791—The Firmware Auto Sync Server Policy is now set to No Actions by default.
  - Old behavior: The Firmware Auto Sync Server Policy was set to Auto Acknowledge by default, which attempted to push the default Host Firmware Package into blades/rack-servers during discovery.
  - New behavior: Withe the Firmware Auto Sync Server Policy set to No Actions by default, you not longer have to manually clear the server information from the database, and re-attempt the discovery/integration.
  - Impact: The customer can now run mixed firmware environments and manage the firmware directly.

- During the creation of a host firmware package, Cisco UCS Manager no longer allows checking or clearing individual components of a blade package or rack package.
  - Old behavior: During creation of a host firmware package, if the customer selects the blade package, or rack package, or both, they can check or clear check boxes associated with any components, but they cannot modify the components of these packages. When they click **Save Changes**, Cisco UCS Manager displays the following error message:

```
Blade Package and/or Rack package is set. Individual PackImage
modification is not allowed for this Host Firmware Package.
```

  - New behavior: Starting with Cisco UCS Manager Release 2.2(6c), during creation of a host firmware package, if the customer selects the blade package, or rack package, or both, all components listed under these packages are grayed out and cannot be selected or cleared. They cannot modify the components of these packages.
  - Impact: The customer will now not be able to check or clear individual components listed under blade or rack packages, if the blade package, or rack package, or both, are selected during creation of a host firmware package.

Release 2.2(5a) introduces the following behavior changes:

- CSCut47053—Support all VIC slots (1,2,4,5) for UCSM-managed single wire management of UCS C240 M4 rack-mount servers.
  - Old behavior: In UCSM mode, single wire management of UCS C240 M4 servers was only supported in Riser 1 slot 2.
  - New behavior: In UCSM mode, single wire management of UCS C240 M4 servers is now supported in Riser 1 (slots 1 and 2) and Riser 2 (slots 4 and 5).
  - Impact: The customer can now insert the VIC in Riser 1 (slots 1 and 2) and Riser 2 (slots 4 and 5) for single wire management of UCS C240 M4 rack servers.

Release 2.2(4b) introduces the following behavior changes:

- Cisco UCS B200 M4, B260 M4, and B460 M4 blade servers no longer support QLogic (UCSB-MEZ-QLG-03) and Emulex (UCSB-MEZ-ELX-03) mezzanine adapter cards.
  - Old behavior: Cisco UCS B200, B260, and B460 M4 servers supported QLogic (UCSB-MEZ-QLG-03) and Emulex (UCSB-MEZ-ELX-03) mezzanine adapter cards with Cisco UCS Manager Release 2.2(3).
  - New behavior: Starting with Cisco UCSM Release 2.2(4b), Cisco UCS B200 M4, B260 M4, and B460 M4 blade servers no longer support QLogic (UCSB-MEZ-QLG-03) and Emulex (UCSB-MEZ-ELX-03) mezzanine adapter cards.
  - Impact: These servers will fail to complete the discovery process if upgraded to Cisco UCS Manager Release 2.2(4b) and later releases.
- CSCus73964—Infrastructure bundle download causes environment to downgrade.
  - Old behavior: Manual upgrade or activation of Cisco UCS Manager, Fabric Interconnects, and IOM was allowed even if the startup version of the default infrastructure bundle was set.
  - New behavior: If the startup version of the default infrastructure bundle is set, manual upgrade or activation of Cisco UCS Manager, Fabric Interconnects, and IOM is not allowed.
  - Impact: To successfully complete a manual upgrade or activation of Cisco UCS Manager, Fabric Interconnects, and IOM, the customer has to make sure that the startup version is cleared before starting manual upgrade or activation. This can be done through the Cisco UCS Manager CLI or the Cisco UCS Manager GUI.

- CSCuq78417—Change reserved VLAN range from 4030 to 4047.
  - Old behavior: The range of reserved VLAN IDs was from 3968 to 4047.
  - New behavior: The range of reserved VLAN IDs is now from 4030 to 4047.
  - Impact: Before downgrading from Cisco UCS Manager Release 2.2(4b), the customer has to make sure that the VLAN IDs from 3968 to 4030 are not user-configured. VLAN IDs from 3968 to 4030 are system-reserved VLAN IDs in earlier releases.

Release 2.2(3a) introduces the following behavior changes:

- CSCup09981—Server reboot was required on FlexFlash disable in Local Disk Configuration Policy.
  - Old behavior: Server reboot was required on FlexFlash disable in Local Disk Configuration Policy.
  - New behavior: Server reboot is no longer required when FlexFlash is disabled in Local Disk Configuration Policy.
  - Impact: Customer has to make sure that the FlexFlash SD cards are not being used by the server before disabling.

Release 2.2(2c) introduces the following behavior changes:

- CSCul74278—Adding or deleting a local storage device in boot policy will cause PNUOS boot irrespective of "Reboot on Update" flag settings.
  - Old behavior: PNUOS boot occurs only when local device is added and SAN device is removed (or vice versa) in boot policy.
  - New behavior: PNUOS boot always occurs after a local storage device is added or removed in boot policy.
  - Impact: This change allows enabling or disabling of the boot BIOS on local storage controller even in the presence of SAN boot devices in boot policy.
- CSCuj81638—The system no longer returns "empty-pool" faults for empty default pools under the root org.
  - Old behavior: When a new system comes online for the first time, "empty-pool " faults get raised for all empty default pools (compute-pool-default, ip-pool-ext-mgmt, ip-pool-iscsi-initiator-pool, mac-pool-default, uuid-pool-default, wwn-pool-default, and wwn-pool-node-default) under the root org. (These fault IDs include F0463, F0464, F0465, F0466, and F0476.)
  - New behavior: An "empty-pool" fault will no longer be raised for any empty default pool under the root org. Instead, the "empty-pool" fault will only be raised for user-generated empty pools.
  - Impact: This change allows default pools to remain empty when user has pools under a created org.

Known Limitations

Known limitations for Cisco UCS Manager 2.2 releases are described in the following sections.

BIOS and BMC Firmware Downgrade

When a new UCS B200 M4 server with the Intel® Xeon® Processor E5-2600 v4 Product Family pre-installed with Cisco UCS Manager Release 2.2(7) firmware is inserted into an existing Cisco UCSM deployment running the Release 2.2(3) infrastructure version, the firmware sync policy, if enabled, will downgrade the BIOS and BMC versions.

The server will fail discovery after the BIOS and BMC versions are downgraded. To recover from this issue, upgrade the BIOS and BMC versions back to the Cisco UCS Manager Release 2.2(7) firmware.

Board Controller Firmware in C-Series Servers

Upgrading board controller firmware in C-Series servers requires a power cycle for the upgrade to take effect.

Cisco UCS Manager Discovery with a QLogic QLE8362 Adapter

The firmware running version on a QLogic QLE8362 adapter that is managed through Cisco UCS Manager must be version 3.50.14 or later. If the firmware running version is earlier than version 3.50.14, discovery will fail. Firmware upgrade must be done out of a standalone Cisco UCS Manager setup.

BIOS and CIMC Firmware Downgrade Restrictions

The following BIOS and CIMC firmware downgrade restrictions were introduced in Cisco UCS Manager Release 2.2(5a):

- For UCS C460 M4 servers with Intel® Haswell processors installed, Cisco UCS Manager prevents the BIOS and CIMC firmware from downgrading to versions earlier than Release 2.2(5a).

The following BIOS and CIMC firmware downgrade restrictions were introduced in Cisco UCS Manager Release 2.2(3a):

- For UCS C22 and C24 M3 servers with Intel® Ivy Bridge processors installed, Cisco UCS Manager prevents the BIOS and CIMC firmware from downgrading to versions earlier than Release 2.2(2a).
- For UCS C220 and C240 M3 servers with Intel® Ivy Bridge processors installed:
  - Cisco UCS Manager prevents the BIOS firmware from downgrading to versions earlier than Release 2.1(3a).
  - Cisco UCS Manager prevents the CIMC firmware from downgrading to versions earlier than Release 2.2(2a).

LAN and SAN Topology Information Limitation

LAN and SAN topology information is available only through XML and CLI. This information is not exposed in the Cisco UCS Manager GUI.

Default Zoning Not Supported in Cisco UCS, Release 2.1(1a) and Later Releases

Default zoning has been deprecated in Cisco UCS, Release 2.1(1a). Cisco has not supported default zoning in Cisco UCS since Cisco UCS, Release 1.4 in April 2011. Fibre Channel zoning, a more secure form of zoning, is available in Cisco UCS, Release 2.1(1a) and later releases. For more information about Fibre Channel zoning, see the Cisco UCS Manager configuration guides for the release to which you are planning to upgrade.

Caution All storage connectivity that relies on default zoning in your current configuration will be lost when you upgrade to Cisco UCS, Release 2.1(1a) or a later release. We recommend that you review the Fibre Channel zoning configuration documentation carefully to prepare your migration before you upgrade to Cisco UCS, Release 2.1(1a) or later. If you have questions or need further assistance, contact Cisco TAC

Cisco UCS Manager Downgrade

Before performing any upgrade or downgrade operation, make sure to perform an all configuration backup of your system. The backup will ensure a seamless downgrade or upgrade, if required.

The following defects are related to downgrade issues:

- CSCul55683 - When downgrading the Cisco UCS Manager image from Release 2.2 to any prior version, you must downgrade Cisco UCS Manager before you downgrade the infrastructure firmware on the FI. If you downgrade the FI first, some FI processes will crash.

  Contact Cisco TAC to recover from this issue.

- CSCuj87553 - If you downgrade the Cisco UCS Manager image from Release 2.2 to any version prior to Release 2.0(4) before the fabric interconnect images are downgraded, the Cisco UCS Manager GUI may not work.

  To recover from this issue, downgrade the kickstart and sytem images on the FI to the same version as the downgraded Cisco UCS Manager image. The Cisco UCS Manager GUI will be able to reconnect successfully after the FI is running the same version as Cisco UCS Manager.

- CSCul54029 - When you downgrade a B22 board controller to 2.1(2) version using auto-install, the activate status shows as failed. Also if you initiate individual board activation, the board control firmware downgrade is blocked.

  To recover from this status, use “force” option to activate the board controller to the same version as the active one. This clears the fault and brings activate status to “Ready”.

Known Limitations and Behaviors

The following known limitations and behaviors are not otherwise documented:

Table 81: Known Limitations in Release 2.2

Defect ID	Symptom	Workaround	First Bundle Affected
CSCus53389	A Cisco UCS B200 M3 blade server running a Cisco UCS Manager version earlier than Release 2.2(3a) with a 32-GB SD memory card (UCS-SD-32G-S) will be able to use only 16 GB memory.	To use the entire capacity of the 32 GB SD memory card, do the following: **1.** Ensure that the CIMC firmware version is Release 2.2(3a) or later **2.** Enable FlexFlash SD card support in a local disk policy **3.** Add the local disk policy to a service profile **4.** Associate the service profile with a server **5.** Create a scrub policy **6.** Add the scrub policy to the service profile **7.** Format the FlexFlash SD cards **8.** Reacknowledge the server **9.** Reacknowledge the server	2.2(1b)B
CSCuu02813	When the network control policy is configured to include all host VLANs, and the number of MAC addresses exceeds 20,000, server discovery fails.	Change the network control policy to include only native VLANs, or reduce the range of allowed VLANs to keep the number of MAC addresses below 20,000.	2.2(4b)A
CSCtq79496	FCoE traffic may experience momentary disruption when system QoS policy is being modified.	This issue has no known work around. To avoid this issue, all QoS policy changes should be made during a maintenance window.	2.0(1m)A

Defect ID	Symptom	Workaround	First Bundle Affected

CSCui95113	Blade discovery fails with the following error:
	`Warning F77960 2013-08-29T17:47:46.044`
	`18211988 [FSM:STAGE:REMOTE-ERROR]: Result: end-point-unavailable Code: unspecified Message: sendSamDmeAdapterInfo: identify failed (sam:dme: ComputeBladeDiscover:NicPresencePeer)`
	`Warning F16520 2013-08-29T17:47:35.122`
	`18211986 [FSM:STAGE:RETRY:]: detect mezz cards in 6/1(FSM-STAGE:sam:dme:ComputeBladeDiscover:`
	`NicPresencePeer)`
		This issue is found when adapters are in DIAG mode.	2.1(2a)B

CSCun25132	On platforms with OOB storage controller, Cisco UCS Manager displays usable (coerced) value in disk inventory section, which is different than the raw 'NumberOfBlocks' value displayed in catalog section.	This is a non-issue; Cisco UCS Manager is designed to report the coerced, or usable, size as reported by the LSI controller. Both the host and OOB interfaces report this same value.	2.2(1b)T
CSCuo14624	When FlexFlash member of dual SD card setup fails and needs to be replaced, the OS needs to be reinstalled, as well.	This issue has no workaround.	2.1(2a)B
CSCup18983	MAC address changes after upgrade from 2.1 to 2.2. **Note** This behavior is expected due to fix for CSCtg93294, which offsets MAC address by 1.	Update MAC security on port with new MAC address. From local-mgmt for each FI, use show mgmt-ip-debug command to find mac address.	2.2(1b)A

Related Documentation

For more information, you can access related documents from the following links:

- Cisco UCS Documentation Roadmap
- Release Bundle Contents for Cisco UCS Software, Release 2.2

Cisco UCS C-Series Rack Mount Server Integration with Cisco UCS Manager

For more information, refer to the related documents available at the following links:

- Cisco UCS C-series Rack Server Integration Guides
- Cisco UCS C-series Software Release Notes