Release Notes for Cisco Intersight Server Firmware 4.3 and 5.2

First Published: 2023-11-15

Last Modified: 2024-04-24

Change in Firmware Version Schema New

- Post Infra Firmware release 4.2(3c):
  - The Server Firmware bundle in IIS will bear the version number in a new
    instead of the letter format.
  - B-Series Server Firmware version number will be in 5.x series

- With Infra Firmware release 4.3(2), the Infra Firmware bundle in IIS will bear
  number in a new format instead of the letter format.

For example : 4.3(2.230117) , where 23 represents year, 0117 shows the increme
number.

Note In IMM Server Firmware bundles prior to the 5.2(0.230040) release, X-Series BIOS images had major versions of 5.0 and 5.1.

Beginning with IMM Server Firmware 5.2(0.230040), the IMM and UCSM BIOS images will be common and numbered beginning with 4.3(2).

The resulting IMM BIOS Image major version sequence will follow 5.0 -> 5.1 -> 4.3 -> so on.

Overview

Cisco Intersight Infrastructure Services (IIS) enable the streamlined deployment, monitoring, management, and support of physical and virtual infrastructure. IIS supports Cisco Unified Computing System™ (UCS) servers and third-party devices. In addition, IIS provides the following advanced management and support capabilities along with global visibility of infrastructure health and status.

- Telemetry data can be analyzed without any manual intervention when a problem occurs.

- Service Request (SR) and a Return Material Authorization (RMA) are raised automatically.

IIS manages the following Cisco UCS servers:

- C-Series Standalone servers
- UCSM Managed Mode (UMM) B-Series, C-Series servers, and X-Series servers (FI-attached)
- Intersight Managed Mode (IMM) B-Series, C-Series, and X-Series servers (FI-attached)

About the Release Notes

This document contains information on new features, resolved caveats, open caveats, and workarounds for following compute node components:

- Adapter
- BIOS
- CIMC
- RAID Controller
- Disk Firmware

This document also includes the following:

- Updated information after the documentation was originally published.
- Related firmware and BIOS on blade, rack, and modular servers and other Cisco Unified Computing System (UCS) components associated with the release.

Revision History

The following table shows the change history for this document.

Revision Date	Description
April 24, 2024	Updated release notes for Cisco UCS C-Series M7 and M6 Server Firmware, Release 4.3(3.240043).

Revision Date	Description
April 17, 2024	Updated the Firmware Version Equivalency Between UCSM and IMM table to include UCS X-Series server version 5.1(1).
	Moved the following 4.3.1 release-specific sections from *Release Notes for Cisco Intersight Server Firmware 4.2, 5.0, and 5.1* to *Release Notes for Cisco Intersight Server Firmware 4.3 and 5.2* (this document): • New Hardware Support in C-Series Firmware 4.3(1.230097) • Resolved Caveats in C-Series M7 Firmware Release 4.3(1.230138) • Resolved Caveats in C-Series M7 Firmware Release 4.3(1.230124) This is to consolidate the 4.3 release information.
March 07, 2024	Updated release notes for Cisco UCS C-Series M7, M6, and M5 Server Firmware, Release 4.3(2.240009).
February 15, 2024	Updated release notes for the following Server Firmware Release versions: • Cisco UCS X-Series M7 Server Firmware, Release 5.2(1.240010) • Cisco UCS X-Series M6 Server Firmware, Release 5.2(1.240010) • Cisco UCS B-Series M6 Server Firmware, Release 5.2(1.240010) • Cisco UCS C-Series M7 and M6 Server Firmware, Release 4.3(3.240022)
January 24, 2024	Updated release notes for the following server firmware release versions: • Cisco UCS X-Series M7 Server Firmware, Release 5.2(0.230127) • Cisco UCS X-Series M6 Server Firmware, Release 5.2(0.230127) • Cisco UCS C-Series M5, M6, and M7 Server Firmware, Release 4.3(2.240002) • Cisco UCS B-Series M5 and M6 Server Firmware, Release 5.2(0.230127)

Revision Date	Description
November 14, 2023	Updated release notes for the following server firmware release versions: • Cisco UCS X-Series M7 Server Firmware, Release 5.2(0.230092) • Cisco UCS X-Series M6 Server Firmware, Release 5.2(0.230092 • Cisco UCS C-Series Server Firmware, Release 4.3(2.230270) • Cisco UCS B-Series Server Firmware, Release 5.2(0.230100)
September 12, 2023	Updated release notes for Cisco UCS X-Series 410c M7 Server Firmware, Release 5.2(0.230061).
August 16, 2023	Created release notes for the following server firmware release versions: • Cisco UCS X-Series M7 Server Firmware, Release 5.2(0.230041) • Cisco UCS X-Series M6 Server Firmware, Release 5.2(0.230040) • Cisco UCS C-Series Server Firmware, Release 4.3(2.230207) • Cisco UCS B-Series Server Firmware, Release 5.2(0.230039)

New Hardware Features in Server Firmware Release

New Hardware Support in C-Series M7 and M6 4.3(3.240043) — None

New Hardware Support in C-Series M7, M6, and M5 4.3(2.240009) — None

New Hardware Support in X-Series M7 Firmware 5.2(1.240010) and C-Series M7 Firmware 4.3(3.240022)

Support for the following 5th Generation Intel® Xeon® Scalable Processors on Cisco UCS X210c M7 servers with Server Firmware release version 5.2(1.240010):

- UCSX-CPU-I8558P - Intel® Xeon® Platinum 8558P Processor
- UCSX-CPU-I8562Y+ - Intel® Xeon® Platinum 8562Y+ Processor
- UCSX-CPU-I8592+ - Intel® Xeon® Platinum 8592+ Processor
- UCSX-CPU-I8568Y+ - Intel® Xeon® Platinum 8568Y+ Processor
- UCSX-CPU-I8592V - Intel® Xeon® Platinum 8592V Processor

- UCSX-CPU-I8580 - Intel® Xeon® Platinum 8580 Processor
- UCSX-CPU-I6542Y - Intel® Xeon® Gold 6542Y Processor
- UCSX-CPU-I6544Y - Intel® Xeon® Gold 6544Y Processor
- UCSX-CPU-I6530 - Intel® Xeon® Gold 6530 Processor
- UCSX-CPU-I6554S - Intel® Xeon® Gold 6554S Processor
- UCSX-CPU-I6548Y+ - Intel® Xeon® Gold 6548Y+ Processor
- UCSX-CPU-I6526Y - Intel® Xeon® Gold 6526Y Processor
- UCSX-CPU-I6534 - Intel® Xeon® Gold 6534 Processor
- UCSX-CPU-I6538Y+ - Intel® Xeon® Gold 6538Y+ Processor
- UCSX-CPU-I6548N - Intel® Xeon® Gold 6548N Processor

Support for the following 5th Generation Intel® Xeon® Scalable Processors on Cisco UCS C220 M7 and C240 M7 servers with Server Firmware version 4.3(3.240022):

- UCS-CPU-I8592V - Intel® Xeon® Platinum 8592V Processor
- UCS-CPU-I8562Y+ - Intel® Xeon® Platinum 8562Y+ Processor
- UCS-CPU-I8568Y+ - Intel® Xeon® Platinum 8568Y+ Processor
- UCS-CPU-I8592+ - Intel® Xeon® Platinum 8592+ Processor
- UCS-CPU-I8558P - Intel® Xeon® Platinum 8558P Processor
- UCS-CPU-I8580 - Intel® Xeon® Platinum 8580 Processor
- UCS-CPU-I8558 - Intel® Xeon® Platinum 8558 Processor
- UCS-CPU-I6542Y - Intel® Xeon® Gold 6542Y Processor
- UCS-CPU-I6544Y - Intel® Xeon® Gold 6544Y Processor
- UCS-CPU-I6548Y+ - Intel® Xeon® Gold 6548Y+ Processor
- UCS-CPU-I6526Y - Intel® Xeon® Gold 6526Y Processor
- UCS-CPU-I6530 - Intel® Xeon® Gold 6530 Processor
- UCS-CPU-I6534 - Intel® Xeon® Gold 6534 Processor
- UCS-CPU-I6554S - Intel® Xeon® Gold 6554S Processor
- UCS-CPU-I6538Y+ - Intel® Xeon® Gold 6538Y+ Processor
- UCS-CPU-I5515+ - Intel® Xeon® Gold 5515+ Processor
- UCS-CPU-I5520+ - Intel® Xeon® Gold 5520+ Processor
- UCS-CPU-I6548N - Intel® Xeon® Gold 6548N Processor
- UCS-CPU-I4514Y - Intel® Xeon® Silver 4514Y Processor
- UCS-CPU-I4516Y+ - Intel® Xeon® Silver 4516Y+ Processor

Supported GPUs

Support for the following GPU cards with the above listed CPUs:

- Support for Data Center GPU Flex 170, FH-3/4L, 150W PCIe on Cisco UCS C240 M7 servers
- Support for Data Center GPU Flex 140, HHHL, 75W PCIe on Cisco UCS C220 M7 and C240 M7 servers

Support for DDR5 5600 MT/s DIMM

Support for the following 5600 DIMMs on Cisco UCS X210c M7 servers with Server Firmware version 5.2(1.240010):

- UCSX-MRX16G1RE3 - 16GB DDR5-5600 RDIMM 1Rx8 (16Gb)
- UCSX-MRX32G1RE3 - 32GB DDR5-5600 RDIMM 1Rx4 (16GB)
- UCSX-MRX64G2RE3 - 64GB DDR5-5600 RDIMM 2Rx4 (16GB)
- UCSX-MRX96G2RF3 - 96GB DDR5-5600 RDIMM 2Rx4 (24GB)
- UCSX-MR128G4RE3 - 128GB DDR5-5600B RDIMM 4Rx4 (16GB)

Support for the following 5600 DIMMs on Cisco UCS C240 M7 and C220 M7 servers with Server Firmware version 4.3(3.240022):

- UCS-MRX16G1RE3 - 16GB DDR5-5600 RDIMM 1Rx8 (16Gb)
- UCS-MRX32G1RE3 - 32GB DDR5-5600 RDIMM 1Rx4 (16Gb)
- UCS-MRX64G2RE3 - 64GB DDR5-5600 RDIMM 2Rx4 (16GB))
- UCS-MRX96G2RF3 - 96GB DDR5-5600 RDIMM 2Rx4 (24GB)
- UCS-MR128G4RE3 - 128GB DDR5-5600 RDIMM 4Rx4 (16GB)

New Hardware Support in B-Series M5 5.2(0.230127) and B-Series M6 Firmware 5.2(1.240010) — None

New Hardware Support in X-Series Firmware 5.2(0.230127), B-Series Firmware 5.2(0.230127), and C-Series Firmware Version 4.3(2.240002) — None

New Hardware Support in X-Series M7 Firmware 5.2(0.230092)

Support for the following Cisco UCS VIC 15000 Series Secure Boot-enabled mLOM adapter on Cisco UCS X-Series servers:

UCSX-ML-V5D200GV2 - Cisco UCS VIC 15230 (2x100G or 4x25G) mLOM on X-Series M6 and M7 servers.

Note The hardware listed above is compatible with Infrastructure firmware version 4.3(2.230129) and later.

For more information on the new Hardware Support, see Supported Hardware for Intersight Managed Mode.

New Hardware Support in X-Series M7 Firmware 5.2(0.230041)

- Support for UCSX-M2-PT-FPN (M.2 NVMe controller) on Cisco UCS X210c M7 Compute Node.
- Support for the following Graphics Processing Units on Cisco UCS X210c M7 and UCS X410c M7 Compute Nodes.
  - UCSC-GPU-H100-80
  - UCSC-GPU-L40
  - UCSC-GPU-L4
  - UCSC-GPU-FLEX140
  - UCSC-GPU-FLEX170

For more information, see Supported Hardware for Intersight Managed Mode.

New Hardware Support in C-Series Firmware 4.3(2.230270)

Support for the following Cisco UCS VIC 15000 Series Secure Boot-enabled mLOM adapters on Cisco UCS C-Series servers:

- UCSC-M-V5D200GV2 - Cisco UCS VIC 15237 (2x40/100/200G) mLOM on C-Series M6 and M7 servers.
- UCSC-M-V5Q50GV2 - Cisco UCS VIC 15427 (4x10/25/50G) mLOM on C-Series M6 and M7 servers.

Note The hardware listed above is compatible with Infrastructure Firmware version 4.3(2.230129) and later.

For more information, see Supported Hardware for Intersight Managed Mode.

New Hardware Support in C-Series Firmware 4.3(2.230207)

- Support for the following Cisco UCS VIC 15000 Series Secure Boot-enabled PCIe adapters on Cisco UCS C-Series M6 and M7 servers:
  - UCSC-P-V5D200G - Cisco UCS VIC 15235 2x40/100/200G
  - UCSC-P-V5Q50G - Cisco UCS VIC 15425 4x10/25/50G

Note The hardware listed above is compatible with Infrastructure Firmware version 4.3(2.230117) and later.

- Support for the following Graphics Processing Units:
  - UCSC-GPU-H100-80 on Cisco UCS C240 M7 server
  - UCSC-GPU-L40 on Cisco UCS C240 M7 server
  - UCSC-GPU-L4 on Cisco UCS C-Series M7 server
  - UCSC-GPU-FLEX140 on Cisco UCS C-Series M7 server

- UCSC-GPU-FLEX170 on Cisco UCS C240 M7 server

For more information, see Supported Hardware for Intersight Managed Mode.

New Hardware Support in C-Series Firmware 4.3(1.230097)

- Support for Cisco UCS C220 M7 and C240 M7 servers.
- Support for the following Graphics Processing Units on C-Series M7 servers:
  - UCSC-GPU-A16
  - UCSC-GPU-A100-80

For more information, see Supported Hardware for Intersight Managed Mode.

Firmware Version Equivalency Between UCSM and IMM

Firmware Version in UCSM	Equivalent Firmware Version of Cisco UCS X-Series Server in IMM
4.2(1)	5.0(1)
4.2(2)	5.0(2)
4.2(3)	5.0(4)
No equivalent firmware version available in UCSM.	5.1(0)
	5.1(1)
4.3(2)	5.2(0)
4.3(3)	5.2(1)

Cross Version Firmware Support

An IMM Server firmware in a domain is supported with a specific IMM Infrastructure firmware version.

The following table shows the supported Server and Infrastructure firmware combinations within an IMM domain. Any additional Infrastructure firmware restrictions are highlighted as a note in the specific New Hardware Support section.

X-Series Server Firmware Version	Infrastructure Firmware Version					
	4.1(3)	4.2(1)	4.2(2)	4.2(3)	4.3(2)	4.3(3)
5.2(1)	N/A	No	No	Yes	Yes	Yes
5.2(0)	N/A	No	No	Yes	Yes	Yes
5.1(1)	N/A	No	No	Yes	Yes	Yes

5.1(0)	N/A	No	No	Yes	Yes	Yes
5.0(4)	N/A	Yes	Yes	Yes	Yes	Yes
5.0(2)	N/A	Yes	Yes	Yes	No	No
5.0(1)	N/A	Yes	Yes	Yes	No	No

C-Series Server Firmware Version	**Infrastructure Firmware Version**					
	4.1(3)	**4.2(1)**	**4.2(2)**	**4.2(3)**	**4.3(2)**	**4.3(3)**
4.3(3)	Yes	Yes	Yes	Yes	Yes	Yes
4.3(2)	Yes	Yes	Yes	Yes	Yes	Yes
4.3(1)	Yes	Yes	Yes	Yes	Yes	Yes
4.2(3)	Yes	Yes	Yes	Yes	Yes	Yes
4.2(2)	Yes	Yes	Yes	Yes	No	No
4.2(1)	Yes	Yes	Yes	Yes	No	No
4.1(3)	Yes	Yes	Yes	Yes	No	No

B-Series Server Firmware Version	**Infrastructure Firmware Version**					
	4.1(3)	**4.2(1)**	**4.2(2)**	**4.2(3)**	**4.3(2)**	**4.3(3)**
5.2(1)	Yes	Yes	Yes	Yes	Yes	Yes
5.2(0)	Yes	Yes	Yes	Yes	Yes	Yes
5.1(0)	Yes	Yes	Yes	Yes	Yes	Yes
4.3(3)	Yes	Yes	Yes	Yes	Yes	Yes
4.3(2)	Yes	Yes	Yes	Yes	Yes	Yes
4.2(3)	Yes	Yes	Yes	Yes	Yes	Yes
4.2(2)	Yes	Yes	Yes	Yes	No	No
4.2(1)	Yes	Yes	Yes	Yes	No	No
4.1(3)	Yes	Yes	Yes	Yes	No	No

Updating the Firmware

To update the Cisco UCS firmware, see Managing Firmware in Intersight Managed Mode

Security Fixes

Security Fixes in C-Series M7 and M6 Firmware Release 4.3(3.240043) — None

Security Fixes in C-Series M7, M6, M5 Firmware 4.3(2.240009) — None

Security Fixes in B-Series M6 5.2(1.240010) and C-Series 4.3(3.240022), X-Series 5.2(1.240010) M6 and M7 Servers

The following security issues are resolved:

Defect ID - CSCwh58728

Cisco UCS Manager includes Third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2023-38408—The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in /usr/lib is not necessarily safe for loading into ssh-agent.)

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Security Fixes in X-Series M6 Server 5.2(0.230127), B-Series Server 5.2(0.230127), and C-Series M6 Server 4.3(2.240002)

The following security issue is resolved:

Defect ID - CSCwh68315

The Cisco products UCS B-Series M6 Servers; UCS C-Series M6 servers; UCS X-Series M6 Compute Nodes include an Intel® CPU that is affected by the vulnerability identified by the following Common Vulnerability and Exposures (CVE) ID:

CVE-2023-23583—Sequence of processor instructions leads to unexpected behavior for some Intel® Processors may allow an authenticated user to potentially enable escalation of privilege and/or information disclosure and/or denial of service via local access.

Security Fixes in C-Series Firmware Release 4.3(2.230270)

The following security issue is resolved:

Defect ID - CSCwh17053

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

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

Defect ID - CSCwh18140

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

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

Security Fixes in C-Series Firmware Release 4.3(2.230207)

The following security issues are resolved:

- **Defect ID - CSCwe96259**

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

  CVE-2023-20228—This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the browser of the targeted user or access sensitive, browser-based information.

- **Defect ID - CSCwf30460**

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

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

- **Defect ID - CSCwf30468**

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

  - CVE-2022-40982—Information exposure through microarchitectural state after transient execution in certain vector execution units for some Intel® Processors may allow an authenticated user to potentially enable information disclosure through local access.
  - CVE-2022-43505—Insufficient control flow management in the BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable denial of service through local access.

Caveats

The open and 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.

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

Resolved Caveats

Resolved Caveats in X-Series Server Firmware

Resolved Caveats in X-Series M7 and M6 Server Firmware Release 5.2(1.240010) — None

Resolved Caveats in X-Series M7 Firmware Release 5.2(0.230127)

The following table lists the resolved caveats in X-Series M7 firmware release 5.2(0.230127)

Defect ID	Description	First Bundle Affected
CSCwh26280	On Cisco UCS X210c M7 servers, when IPMI tool sends a query to the out-of-band (OOB) IP address for the server, it takes more than 30 seconds to receive a response. This delay causes monitoring tools to display an error because the expected response time in less than 30 seconds.	5.1(0.230075)

Resolved Caveats in X-Series M7 Firmware Release 5.2(0.230092)

The following table lists the resolved caveats in X-Series M7 firmware release 5.2(0.230092)

Defect ID	Description	First Bundle Affected
CSCwh28307	After upgrading the X210cM7 or X410c M7 servers to version 5.2(0.230041), VIC techsupport files were not included in the techsupport package.	5.1(0.230075)

Resolved Caveats in X-Series M7 Firmware Release 5.2(0.230061)

The following table lists the resolved caveats in X-Series 410c M7 firmware release 5.2(0.230061)

Defect ID	Description	First Bundle Affected
CSCwh42695	Platform ID for Cisco UCS X410c M7 Compute Node appears incorrect in two boards as X210c M7 ID 0x84 instead of 0x85.	5.2(0.230041)
CSCwd97069	In Cisco UCS X410c M7 Compute Node, with PXE boot policy enable MK-TME and disable the CPU PA limit. Try to boot into the OS. It is observed that the Compute Node cannot boot into W2K22 and RHEL8.2.	5.2(0.230041)
CSCwh10938	SPR PLR3 OOB MCC SKU S3 stepping fix is required for Cisco UCS X410c M7 Compute Node.	5.2(0.230041)
CSCwf99117	Optimized Power Mode token is enabled in Cisco UCS X410c M7 Compute Node. It is observed that C1E is disabled.	5.2(0.230041)

Resolved Caveats in X-Series M6 Firmware Release 5.2(0.230127)

The following table lists the resolved caveats in X-Series M6 firmware release 5.2(0.230127)

Defect ID	Description	First Bundle Affected
CSCwi50991	The Cisco UCS X210c M6 servers, operating on the server firmware version 5.2(0.230040), encountered a critical issue wherein the Watchdog Baseboard Management Controller (BMC) experienced persistent crashes, impeding server stability.	5.2(0.230040)

Resolved Caveats in X-Series M6 Firmware Release 5.2(0.230040)

The following table lists the resolved caveats in X-Series M6 firmware release 5.2(0.230040)

Defect ID	Description	First Bundle Affected
CSCwe87623	In all models of M6 servers, it is observed that with every power cycle, there is latency in generic inventory Information update as a result HCL status appears Incomplete. The genericInventory mo entries get deleted and inserted completely. During this update of the inventory info, missing OS information results in momentary invalidation of HCL status until OS is booted.	5.0(2b)
CSCwf23487	Server discovery fails after firmware upgrade for Cisco UCS X-Series M6 Compute Node.	5.1(0.230054)

Resolved Caveats in C-Series Server Firmware

Resolved Caveats in C-Series M7 and M6 Firmware Release 4.3(3.240043) — None

Resolved Caveats in C-Series M7, M6, and M5 Server Firmware, Release 4.3(2.240009)

The following table lists the resolved caveats in C-Series firmware release 4.3(2.240009)

Defect ID	Description	First Bundle Affected
CSCwj00617	In Cisco UCS C-Series M5 and M6 servers, the SAS expander firmware update from the XML API interface, using HTTP and TFTP protocol, fails and displays the following error message: `Operation failed. Invalid Password!`	4.2(3i)
CSCwi97945	In Cisco UCS M5 and M6 servers, the SAS expander firmware update from the Cisco Integrated Management Controller (CLI) interface, using HTTP and TFTP protocol, fails and displays the following error message: `Operation failed. Invalid Password!`	4.2(3i)

Resolved Caveats in C-Series Firmware Release 4.3(2.240002)

The following table lists the resolved caveats in C-Series firmware release 4.3(2.240002)

Defect ID	Description	First Bundle Affected
CSCwh53073	On Cisco UCS C240 M5 SD and Cisco UCS C245 M6 SX, the alarms generated from Cisco Integrated Management Controller (CIMC) are not accurately represented in Intersight User Interface (UI). The Alarm page in the Intersight UI displayed the date/time of the associated alarm as 'in 9 hours' though the alarm was triggered immediately after the event.	4.2(2a)
CSCwi04192	On Cisco UCS C220 M6 and C240 M6 servers, the third-party Mellanox MLOM cards (Mellanox UCSC-O-N6CD100GF) are prone to overheating and link flapping due to the default fan policy failing to offer adequate cooling and required fan speed alteration settings to cool the card.	4.3(2b)C

Resolved Caveats in C-Series Firmware Release 4.3(2.230270)

The following table lists the resolved caveats in C-Series firmware release 4.3(2.230270)

Defect ID	Description	First Bundle Affected
CSCwh34432	While mounting vMedia using Redfish API, when the user forgets to post the TransferProtocolType field, the following error message is displayed: `Message: Bad request format`	4.3.1.230097
CSCwf44478	In Cisco UCS C-series M7 servers with Red Hat Enterprise Linux OS versions 8.6 and 9.0, Micron 7450 NVMe drive does not get detected after hot-plug.	4.3.2.230207
CSCwh13701	When Cisco UCS C225 M6 and C245 M6 servers, equipped with power supply units (PSUs) and have firmware versions prior to 4.2(3h), the servers may power off unexpectedly without any warning.	4.3.1.230097
CSCwf94278	In Cisco UCS C-series M5 servers with release versions 4.1(3b), 4.2(2a), 4.2(3b), the user can create a session with a 'read only' user, but unable to delete or log out from the session while using the Redfish API interface.	4.2(2a)

Resolved Caveats in C-Series Firmware Release 4.3(2.230207)

The following table lists the resolved caveats in C-Series firmware release 4.3(2.230207)

Defect ID	Description	First Bundle Affected
CSCwe19822	In all models of M5 servers, it is observed that CIMC reset occurs due to kernel crash and watchdog reset.	4.2(2f)

Defect ID	Description	First Bundle Affected
CSCwe87623	In all models of M6 servers, it is observed that with every power cycle, there is latency in generic inventory Information update as a result HCL status appears Incomplete. The genericInventory mo entries get deleted and inserted completely. During this update of the inventory info, missing OS information results in momentary invalidation of HCL status until OS is booted.	4.2(3e)

Resolved Caveats in C-Series M7 Firmware Release 4.3(1.230138)

The following table lists the resolved caveats in C-Series M7 firmware release 4.3(1.230138)

Defect ID	Description	First Bundle Affected
CSCwe87764	In Cisco UCS M7 servers equipped with 128GB DIMMs, there might be a decrease in the performance of the CPU when the values of the voltage regulator is modified to enhance the system performance.	4.3(1.230124)

Resolved Caveats in C-Series M7 Firmware Release 4.3(1.230124)

The following table lists the resolved caveats in C-Series M7 firmware release 4.3(1.230124)

Defect ID	Description	First Bundle Affected
CSCwe47118	Redfish monitor core occured during combinational stress(Redfish stress included).	4.3(1.230097)

Resolved Caveats in B-Series Server Firmware

Resolved Caveats in B-Series M6 5.2(1.240010) and M5 5.2(0.230127) Firmware Release — None

Resolved Caveats in B-Series Firmware Release 5.2(0.230127) — None

Resolved Caveats in B-Series Firmware Release 5.2(0.230039)

The following table lists the resolved caveats in X-Series M6 firmware release 5.2(0.230039)

Defect ID	Description	First Bundle Affected
CSCwe00937	Cisco UCS B200 M6 servers respond to SSH requests but have Serial Over LAN (SOL) disabled. As hmac-sha1 are enabled for SSH, the CIMC IPs get flagged as vulnerable in the security scans.	4.2(2d)
CSCwe19822	In all models of M5 servers, it is observed that CIMC reset occurs due to kernel crash and watchdog reset.	4.2(2e)

Defect ID	Description	First Bundle Affected
CSCwe87623	In all models of M6 servers, it is observed that with every power cycle, there is latency in generic inventory Information update as a result HCL status appears Incomplete. The genericInventory mo entries get deleted and inserted completely. During this update of the inventory info, missing OS information results in momentary invalidation of HCL status until OS is booted.	5.1(0.230069)
CSCwf02413	For Cisco UCS B200 M6 server, Power Budget alert is observed on an unassociated server. Alert clears on its own if server is not associated with a server profile and if discovery is successful.	4.2(2d)

Open Caveats

Open Caveats in C-Series M7 and M6 Firmware Release 4.3(3.240043) — None

Open Caveats in C-Series M7, M6, and M5 Firmware 4.3(2.240009) — None

Open Caveats in X-Series M7 Firmware Release 5.2(1.240010) — None

Open Caveats in C-Series Firmware Release 4.3(3.240022)

The following table lists the open caveats in C-Series firmware release 4.3(3.240022)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwi85031	Cisco UCS C240 M7 server with an Emerald Rapids 8558+, 8568Y+ or CPU SKUs processor and two Intel Flex 170 GPUs, experienced a crash and failed to load the RHEL 9.2 or Ubuntu 22.04.3. Instead of successfully booting and installing the OS, the system hung and crashed.	1. Access the BIOS setup. 2. Navigate Advanced > Socket Configuration > Uncore Configuration > Uncore General Configuration. 3. Change MMIO High Granularity Size to **1024G** and Press **F10**to save. 4. Reboot the server.	4.3(3.240022)
CSCwi85033	Cisco UCS C240 M7 server with an Emerald Rapids 8558+, 8568Y+ or CPU SKUs processor and two NVDIA H100 GPUs, experienced a crash and failed to load the RHEL 9.2 or Ubuntu 22.04.3, led to operational disruptions.	1. Access the BIOS setup. 2. Navigate Advanced > Socket Configuration > Uncore Configuration > Uncore General Configuration. 3. Change MMIO High Granularity Size to **1024G** and Press **F10**to save. 4. Reboot the server.	4.3(3.240022)

Open Caveats in X-Series M7 Firmware Release 5.2(0.230127) — None

Open Caveats in X-Series M6 Firmware Release 5.2(0.230127) — None

Open Caveats in C-Series M7 Firmware Release 4.3(2.240002) — None

Open Caveats in B-Series M5 Firmware Release 5.2(0.230127) and M6 Firmware Release 5.2(1.240010) — None

Related Documentation

- Release Notes and Release Bundles for Cisco Intersight
- Release Notes for Cisco UCS Manager
- Release Notes for Cisco UCS Rack Server Software