Release Notes for Cisco Intersight Server Firmware 4.2, 5.0, and 5.1

First Published: 2023-09-29

Last Modified: 2024-10-01

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.

Related Documentation

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

Revision History

The following table shows the online change history for this document.

Revision Date	Description
October 01, 2024	Cisco UCS X-Series 5.0(4g), C-Series 4.2(3m), and B-Series 4.2(3j) Server Firmware versions have been released. This release includes updates to the Security Fixes in C-Series Release 4.2(3m) and Resolved Caveats in Release 4.3(3m) sections. It does not include any new hardware support or open caveats.

Revision Date	Description
June 17, 2024	Cisco UCS X-Series 5.0(4f), C-Series 4.2(3l), and B-Series 4.2(3i) Server Firmware versions have been released. This release includes updates to the Security Fixes in C-Series Release 4.2(3l) and Resolved Caveats in C-Series M5 and M6 Firmware Release 4.2(3l) sections. It does not include any new hardware support or open caveats.
April 17, 2024	Updated the **Firmware Version Equivalency Between UCSM and IMM** table to add 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* (this document) to *Release Notes for Cisco Intersight Server Firmware 4.3 and 5.2*: • 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.
February 22, 2024	Cisco UCS C-Series Server Firmware version 4.2(3j) has been released. This release includes updates to the Security Fixes in Release 4.2(3j) and Resolved Caveats in X-Series M7 and M6 Firmware Release 4.2(3j) sections. It does not include any new hardware support or open caveats.
November 07, 2023	Updated release notes for Cisco UCS C-Series Server Firmware, Release 4.2(3i)
September 29, 2023	Updated release notes for Cisco UCS C-Series Server Firmware, Release 4.2(3h)
Aug 08, 2023	Updated release notes for Cisco UCS C-Series Server Firmware, Release 4.2(3g)
June 08, 2023	Updated release notes for Cisco UCS X-Series M7 Server Firmware, Release 5.1(1.230052)
June 06, 2023	Updated release notes for Cisco UCS C-Series M7 Server Firmware, Release 4.3(1.230138)
April 12, 2023	Updated release notes for Cisco UCS C-Series M7 Server Firmware, Release 4.3(1.230124)
March 31, 2023	Updated release notes for Cisco UCS X-Series M7 Server Firmware, Release 5.1(0.230122), Cisco UCS X-Series M6 Server Firmware, Release 5.1(0.230075), Cisco UCS B-Series M6 Server Firmware, Release 5.1(0.230069), and Cisco UCS B-Series M5 Server Firmware, Release 5.1(0.230073).

Revision Date	Description
March 16, 2023	Updated release notes for Cisco UCS X-Series M7 Server Firmware, Release 5.1(0.230096), Cisco UCS X-Series M6 Server Firmware, Release 5.1(0.230054), Cisco UCS C-Series Server Firmware, Release 4.3(1.230097), Cisco UCS B-Series M5 Server Firmware, Release 5.1(0.230054), and Cisco UCS B-Series M6 Server Firmware, Release 5.1(0.230052).
January 10, 2023	Updated release notes for Cisco UCS X-Series Server Firmware, Release 5.0(4a)
November 29, 2022	Updated release notes for Cisco UCS X-Series Server Firmware, Release 5.0(2e)
September 20, 2022	Updated release notes for Cisco UCS X-Series Server Firmware, Release 5.0(2d)
September 01, 2022	Updated release notes for Cisco UCS X-Series Server Firmware, Release 5.0(1f)
July 21, 2022	Updated release notes for Cisco UCS X-Series Server Firmware, Release 5.0(2b)
June 16, 2022	Updated release notes for Cisco UCS X-Series Server Firmware, Release 5.0(1e)
February 15, 2022	Created release notes for Cisco UCS X-Series Server Firmware, Release 5.0(1c).

New Software Support

Intersight software features may not align with the Intersight firmware release schedule. To know more about the latest software features, see the What's New section in Intersight Help Center.

New Features in Release

New Hardware Features in Server Firmware Releases

New Hardware Support in X-Series 5.0(4g), C-Series 4.2(3m), and B-Series 4.2(3j) Firmware — None

New Hardware Support in X-Series 5.0(4f), C-Series 4.2(3l), and B-Series 4.2(3i) Firmware — None

New Hardware Support in X-Series M7 Firmware 5.1(1.230052)

Cisco UCS X410c M7 Compute Node

The Cisco UCS X410c M7 Compute Node is the first 4-socket 4th Gen Intel® Xeon® Scalable Processors computing device to integrate into the Cisco UCS X-Series Modular System. Up to four compute nodes or two compute nodes and two GPU nodes can reside in the 7-rack-unit (7RU) Cisco UCS X9508 Server Chassis, offering high performance and efficiency gains for a wide range of mission-critical enterprise applications, memory-intensive applications and bare-metal and virtualized workloads.

The Cisco UCS X410c M7 provides these main features:

- CPU: Four 4th Gen Intel Xeon Scalable Processors with up to 60 cores per processor.
- Memory: Up to 16TB of main memory with 64x 256 GB DDR5-4800 Memory DIMMs.
- Storage: Up to six hot-pluggable solid-state drives (SSDs), or non-volatile memory express (NVMe) 2.5-inch drives with a choice of enterprise-class RAID or passthrough controllers, up to two M.2 SATA drives with optional hardware RAID.
- mLOM virtual interface card:
  - Cisco UCS VIC 15420 occupies the server's modular LAN on motherboard (mLOM) slot, enabling up to 50 Gbps of unified fabric connectivity to each of the chassis's intelligent fabric modules (IFMs) for 100 Gbps connectivity per server.
  - Cisco UCS VIC 15231 occupies the server's modular LAN on motherboard (mLOM) slot, enabling up to 100 Gbps of unified fabric connectivity to each of the chassis's intelligent fabric modules (IFMs) for 100 Gbps connectivity per server.
- Optional mezzanine virtual interface card:
  - Cisco UCS 5th Gen VIC 15422 can occupy the server's mezzanine slot at the bottom rear of the chassis. This card's I/O connectors link to Cisco UCS X-Fabric technology. An included bridge card extends this VIC's 2x 50 Gbps of network connections through IFM connectors, bringing the total bandwidth to 100 Gbps per fabric (for a total of 200 Gbps per server).
  - Cisco UCS PCI Mezz card for Cisco UCS X-Fabric can occupy the server's mezzanine slot at the bottom rear of the chassis. This card's I/O connectors link to Cisco UCS X-Fabric modules and enable connectivity to the Cisco UCS X440p PCIe Node.
  - All VIC mezzanine cards also provide I/O connections from the X410c M7 compute node to the X440p PCIe node.
- Security: The server supports an optional trusted platform module (TPM). Additional features include a secure boot FPGA and ACT2 anti-counterfeit provisions.

Note Cisco UCS X410c M7 Compute Node requires Infrastructure firmware version 4.2(3e) or later

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

New Hardware Support in X-Series Firmware 5.1(0.230096)

Support for the following:

- **Cisco UCS X210c M7 Compute Node**

  The Cisco UCS X210c M7 Compute Node is the second generation of compute node to integrate into the Cisco UCS X-Series Modular System. Up to eight compute nodes can reside in the 7-rack-unit (7RU) Cisco UCS X9508 Server Chassis, offering one of the highest densities of compute, I/O, and storage per rack unit in the industry.

  The Cisco UCS X210c M7 provides these main features:

- CPU: Up to 2x 4th Gen Intel® Xeon® Scalable Processors with up to 60 cores per processor and upto 2.625 MB Level 3 cache per core and up to 112.5 MB per CPU.
- Memory: Up to 8TB of main memory with 32x 256 GB DDR5-4800 DIMMs.
- Storage: Up to six hot-pluggable, Solid-State Drives (SSDs), or Non-Volatile Memory express (NVMe) 2.5-inch drives with a choice of enterprise-class Redundant Array of Independent Disks (RAIDs) or passthrough controllers, up to two M.2 SATA drives with optional hardware RAID.
- Optional front mezzanine GPU module: The Cisco UCS front mezzanine GPU module is a passive PCIe Gen 4.0 front mezzanine option with support for up to two U.2 NVMe drives and two HHHL GPUs.
- mLOM virtual interface card: Cisco UCS Virtual Interface Card (VIC) 15420 occupies the server's modular LAN on motherboard (mLOM) slot, enabling up to 50 Gbps of unified fabric connectivity to each of the chassis intelligent fabric modules (IFMs) for 100 Gbps connectivity per server.

  Cisco UCS Virtual Interface Card (VIC) 15231 occupies the server's modular LAN on motherboard (mLOM) slot, enabling up to 100 Gbps of unified fabric connectivity to each of the chassis intelligent fabric modules (IFMs) for 100 Gbps connectivity per server.
- Optional mezzanine card: Cisco UCS 5th Gen Virtual Interface Card (VIC) 15422 can occupy the server's mezzanine slot at the bottom rear of the chassis. This card's I/O connectors link to Cisco UCS X-Fabric technology. An included bridge card extends this VIC's 2x 50 Gbps of network connections through IFM connectors, bringing the total bandwidth to 100 Gbps per fabric (for a total of 200 Gbps per server).

  Cisco UCS PCI Mezz card for X-Fabric can occupy the server's mezzanine slot at the bottom rear of the chassis. This card's I/O connectors link to Cisco UCS X-Fabric modules and enable connectivity to the Cisco UCS X440p PCIe Node.

  All VIC mezzanine cards also provide I/O connections from the X210c M7 compute node to the X440p PCIe Node.

- Support for the following Cisco UCS 15000 Series VIC adapters:
  - UCSX-ML-V5Q50G - Cisco UCS VIC 15420 4x25G mLOM adapter for Cisco UCS X210c M7 Compute Nodes.
  - UCSX-ME-V5Q50G - Cisco UCS VIC 15422 4x25G mezz for Cisco UCS X210c M7 Compute Nodes.

Note UCSX-210C-M7 Compute Node requires Cisco Intersight Infrastructure Firmware version 4.2(3b) or above.

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

New Hardware Support in X-Series Firmware 5.1(0.230054)

Support for the following Cisco UCS 15000 Series VIC adapters:

- UCSX-ML-V5Q50G - Cisco UCS VIC 15420 4x25G mLOM adapter for Cisco UCS X210c M6 Compute Node.
- UCSX-ME-V5Q50G - Cisco UCS VIC 15422 4x25G mezz for Cisco UCS X210c M6 Compute Node.

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

New Hardware Support in X-Series Firmware 5.0(4b)

Catalog support for the following on Cisco UCS X210c M6 Compute Node:

- KIOXIA PM7 1.9TB/3.8TB/7.6TB/15TB (1DWPD) SED
- Micron 5400 1DWPD SATA SSD 960GB/1.9TB/480GB
- Micron 5400 1DWPD 3.8TB and 7.6TB SSD SED
- Micron 5400 240GB, 480GB, 960GB M.2 SSD
- Micron 128GB,32GB DIMM

New Hardware Support in X-Series Firmware 5.0(2e)

Support for the following Graphics Processing Units on UCSX-440P with Cisco UCS X210c M6 Compute Node:

- UCSX-GPU-A100-80

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

New Hardware Support in X-Series Firmware 5.0(2d)

Support for the following Graphics Processing Units on UCSX-440P with Cisco UCS X210c M6 Compute Node:

- UCSX-GPU-T4-16
- UCSX-GPU-A40
- UCSX-GPU-A16

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

New Hardware Support in X-Series Firmware 5.0(2b)

Support for the following:

- Support for UCSX-ML-V5D200G modular LAN on motherboard (mLOM) adapter on Cisco UCS X210c M6 Compute Node.

Note Cisco UCS VIC 15231 (UCSX-ML-V5D200G) requires Infrastructure firmware version 4.2(2) or later that contains VIC firmware 5.2(2)

- Support for Front Mezz (UCSX-X10C-GPUFM) for Cisco UCSX-210C-M6 servers.
- Support for NVIDIA T4 GPU (UCSX-GPU-T4-MEZZ) for Cisco UCSX-210C-M6 servers.
- Support for Cisco UCSX-440P PCIe Node.

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

New Hardware Support in X-Series Firmware 5.0(1c)

Catalog support for the following on Cisco UCS X210c M6 Compute Node :

- UCS-SD76TBKNK9 (7.6TB 2.5 inch Enterprise value 12G SAS SSD (1DWPD, SED-FIPS)
- UCS-SD480G63X-EP (480GB 2.5in Enterprise performance 6GSATA SSD)
- UCS-SD480G6I1X-EV (480GB 2.5 inch Enterprise Value 6G SATA SSD)
- UCS-SD800GS3X-EP (800GB 2.5in Enterprise Performance 12G SAS SSD)
- UCS-SD19TS1X-EV (1.9TB 2.5 inch Enterprise Value 12G SAS SSD
- UCS-SD960G6S1X-EV (960GB 2.5 inch Enterprise Value 6G SATA SSD)

New Hardware Support in X-Series Firmware 5.0(1b)

Cisco UCS X210c M6 Compute Node

The Cisco UCS X210c M6 Compute Node is the first computing device to integrate into the Cisco UCS X-Series Modular System. Up to eight compute nodes can reside in the 7-Rack-Unit (7RU) Cisco UCS X9508 Chassis, offering one of the highest densities of compute, I/O, and storage per rack unit in the industry.

The Cisco UCS X210c M6 provides these main features:

- CPU: Up to 2x 3rd Gen Intel® Xeon® Scalable Processors with up to 40 cores per processor and 1.5 MB Level 3 cache per core.
- Memory: Up to 32x 256 GB DDR4-3200 DIMMs for up to 8 TB of main memory. Configuring up to 16x 512-GB Intel Optane™ persistent memory DIMMs can yield up to 12 TB of memory.
- Storage: Up to six hot-pluggable, Solid-State Drives (SSDs), or Non-Volatile Memory express (NVMe) 2.5-inch drives with a choice of enterprise-class Redundant Array of Independent Disks (RAIDs) or passthrough controllers with four lanes each of PCIe Gen 4 connectivity and up to 2 M.2 SATA drives for flexible boot and local storage capabilities.
- mLOM virtual interface card: The Cisco UCS Virtual Interface Card (VIC) 14425 can occupy the server's modular LAN on motherboard (mLOM) slot, enabling up to 50 Gbps of unified fabric connectivity to each of the chassis Intelligent Fabric Modules (IFMs) for 100 Gbps connectivity per server.
- Optional mezzanine virtual interface card: Cisco UCS Virtual Interface Card (VIC) 14825 can occupy the server's mezzanine slot at the bottom of the chassis. This card's I/O connectors link to Cisco UCS X-Fabric Technology that is planned for future I/O expansion. An included bridge card extends this VIC's 2x 50 Gbps of network connections through IFM connectors, bringing the total bandwidth to 100 Gbps per fabric—a total of 200 Gbps per server.

Note Cisco UCS Virtual Interface Card (VIC) 14425/14825 requires Infrastructure firmware version 4.2(1) or later

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

New Hardware Support in C-Series Firmware 4.2(3j) — None

New Hardware Support in C-Series Firmware 4.2(3b)

- Support for the following Graphics Processing Units in Intersight Managed Mode:
  - UCSC-GPU-A16 on Cisco UCS C-Series M6 server
  - UCSC-GPU-A100-80 on Cisco UCS C-Series M5 and M6 servers

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

New Hardware Support in C-Series Firmware 4.2(2g)

- Support for the following Cisco UCS VIC 1300 Series adapters on C-Series M5 servers.
  - UCSC-PCIE-C40Q-03
  - UCSC-MLOM-C40Q-03

Note Cisco UCS VIC 1300 Series adapters require VIC firmware version 4.5(2d) or above.

- Catalog support for the following:
  - Intel/Solidigm S4520, S4620 and S4520 M.2 SATA FW 7CV1CS02 for C220, C240, C480 M5 servers and C220, C240 M6 servers.
  - Samsung 256GB Octal Rank 3200 LRDIMM for C-Series M5 servers in IMM.

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

New Hardware Support in C-Series Firmware 4.2(1j)

Catalog support for the following:

- Micron 64GB RDIMM DRx4 3200 (16Gb) 1anm Z42B on C-series M5 and M6 servers in Intersight Managed Mode.
- Seagate Evans BP 12TB and 18TB SAS 4k on C220 and C240 M6 servers.
- Hynix 128GB LRDIMM QRx4 3200 (16Gb, DDP) 1znm (C-die) for C-Series M5 and M6 servers.
- Micron 5300 1.9TB M.2 SSD on C220 and C240 M6 servers
- WD Paris-D 20TB drive on C220 and C240 M6 servers
- Samsung PM893 EnterpriseValue SATA SFF 960GB,1.9T,3.8T,7.6T(1DWPD)(00AK1) on C220 and C240 M6 servers.

New Hardware Support in C-Series Firmware 4.2(1g)

Catalog support for the following:

- A16 PID on C225 and C245 M6 servers

- WD Leo-B He 14TB 4k SAS LFF (MID M6) on C220 and C240 M6 servers
- WD Vela-AX 10TB 12G SAS 7.2K RPM LFF HDD (4K) (MID M6) on C220 and C240 M6 servers
- Toshiba MG07 14TB 12G SAS 4k ISE (MID M6) on C220 and C240 M6 servers.
- Seagate Skybolt V6 NAND-1.8TB(4k) & 2.4TB (4k) SED-FIPS on C-Series M6 servers
- Samsung PM893 EnterpriseValue SATA SFF 960GB,1.9T,3.8T,7.6T(1DWPD)(00AK1) on C220 and C240 M6 servers.

New Hardware Support in C-Series Firmware 4.2(1f)

Catalog support for the following:

- Samsung 256GB Octal Rank 3200 LRDIMM on C245 M6 servers
- Micron 5200 1X 3.8TB on C-Series M6 servers
- Micron 32GB RDIMM DRx4 3200 (8Gb) 1anm Z41C on C-Series M6 servers
- Samsung 32GB RDIMM DRx4 3200 (8Gb) D1z and 16GB RDIMM SRx4 3200 (8Gb) D1y on C-Series M6 servers
- Hynix 64GB RDIMM DRx4 3200 (16Gb) 1znm and 16GB RDIMM SRx4 3200 1ynm (8Gb) on C-Series M6 servers.

New Hardware Support in B-Series Firmware 4.2(2e)

- Support for the following Cisco UCS VIC 1300 Series adapters on B-Series M5 servers.
  - UCSB-MLOM-40G-03
  - UCSB-VIC-M83-8P
  - UCSB-MLOM-PT-01

Note Cisco UCS VIC 1300 Series adapters require VIC firmware version 4.5(2d) or above.

- Catalog support for the following:
  - FW E201CP07 for Coldstream 375G new media type on B-Series M5 servers in Intersight Managed Mode.
  - FW 7CV1CS02 for Solidigm S4520 YVRR SATA 240GB/960GB/3.8TB on B-Series M5 and M6 servers.
  - Seagate Cooper - 7.6TB (1DWPD) on B-Series M5 and M6 servers.

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

Firmware Version Equivalency Between Cisco Intersight, Cisco IMC, and Cisco UCS Manager

For more information, see Cisco UCS Equivalency Matrix for Cisco Intersight, Cisco IMC, and Cisco UCS Manager.

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**		
	4.2(1)	**4.2(2)**	**4.2(3)**
5.1(1)	No	No	Yes
5.1(0)	No	No	Yes
5.0(4)	Yes	Yes	Yes
5.0(2)	Yes	Yes	Yes
5.0(1)	Yes	Yes	Yes

C-Series Server Firmware Version	**Infrastructure Firmware Version**		
	4.2(1)	**4.2(2)**	**4.2(3)**
4.3(1)	Yes	Yes	Yes
4.2(3)	Yes	Yes	Yes
4.2(2)	Yes	Yes	Yes
4.2(1)	Yes	Yes	Yes
4.1(3)	Yes	Yes	Yes

B-Series Server Firmware Version	**Infrastructure Firmware Version**		
	4.2(1)	**4.2(2)**	**4.2(3)**
5.1(0)	Yes	Yes	Yes
4.2(3)	Yes	Yes	Yes
4.2(2)	Yes	Yes	Yes
4.2(1)	Yes	Yes	Yes
4.1(3)	Yes	Yes	Yes

Updating the Firmware

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

Security Fixes

Security Fixes in C-Series Release 4.2(3m)

The following security issues are resolved:

Defect ID - CSCwk77757

Cisco UCS C-Series M5 servers includes Third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- **CVE-2024-24853**—Incorrect behavior order in transition between executive monitor and SMI Transfer Monitor (STM) in some Intel(R) Processor may allow a privileged user to potentially enable escalation of privilege through local access.
- **CVE-2024-21781**—Improper input validation in UEFI firmware for some Intel(R) Processors may allow a privileged user to enable information disclosure or denial of service through through local access.

Defect ID - CSCwk62266

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

- **CVE-2024-6387**—A race condition has been identified in the sshd service related to its signal handler. If a client fails to authenticate within the LoginGraceTime period (default is 120 seconds, previously 600 seconds in older OpenSSH versions), the sshd SIGALRM handler is triggered asynchronously. This handler, however, invokes several functions that are not safe to call from within a signal handler, such as syslog().

Security Fixes in X-Series Release 5.0(4g) and B-Series Release 4.2(3j) — None

Security Fixes in C-Series Release 4.2(3l)

The following security issues are resolved:

Defect ID - CSCwi59840

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

- **CVE-2023-48795**—The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks, such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, also known as Terrapin attack.

  This occurs because theSSH BinaryPacketProtocol (BPP), implemented by these extensions, mishandles the handshake phase and use ofsequence numbers.For example, when there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC), the bypass occurs in chacha20-poly1305@openssh.com, (and if CBC is used, then the -etm@openssh.com MAC algorithms).

Security Fixes in X-Series Release 5.0(4f) and B-Series Release 4.2(3i) — None

Security Fixes in Release 4.2(3j)

The following security issues are resolved:

Defect ID - CSCwh58728

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

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 Release 5.1(0.230054)

The following security issues are resolved:

Defect ID — CSCwd07517

Cisco UCS X-Series M6 Compute Nodes include third-party software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2021-23017 - A security issue in nginx resolver which might allow an attacker who is able to forge UDP packets from the DNS server to cause 1-byte memory overwrite, resulting in worker process crash or potential other impact.
- CVE-2021-3618 - A MiTM attacker having access to victim's traffic at the TCP/IP layer can redirect traffic from one subdomain to another, resulting in a valid TLS session.

Defect ID — CSCwd10018

Cisco UCS X-Series M6 Compute Nodes include third-party software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2021-39537 - An issue was discovered in ncurses through v6.2-1. _nc_captoinfo in captoinfo.c has a heap-based buffer overflow.
- CVE-2022-29458 - ncurses 6.3 before patch 20220416 has an out-of-bounds read and segmentation violation in convert_strings in tinfo/read_entry.c in the terminfo library.

Security Fixes in Release 5.0(1f)

The following security issues are resolved:

Defect ID—CSCwb67158

Cisco UCS B-Series M4 Blade Servers (except B260, B460) and Cisco UCS C-Series M4 Rack Servers (except C460) include an Intel® Processor that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID(s):

- CVE-2021-0153—Out-of-bounds write in the BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable escalation of privilege through local access.
- CVE-2021-0154—Improper input validation in the BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable escalation of privilege through local access.
- CVE-2021-0155—Unchecked return value in the BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable information disclosure through local access.
- CVE-2021-0190—Uncaught exception in the BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable escalation of privilege through local access.
- CVE-2021-33123—Improper access control in the BIOS authenticated code module for some Intel® Processors may allow a privileged user to potentially enable escalation of privilege through local access.
- CVE-2021-33124—Out-of-bounds write in the BIOS authenticated code module for some Intel® Processors may allow a privileged user to potentially enable escalation of privilege through local access.

Defect ID—CSCwb67159

Cisco UCS B-Series M5 Blade Servers and Cisco UCS C-Series M5 Rack Servers include an Intel® processor that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID(s):

- CVE-2021-0189—Use of out-of-range pointer offset in the BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable aescalation of privilege through local access.
- CVE-2021-0159—Improper input validation in the BIOS authenticated code module for some Intel® Processors may allow a privileged user to potentially enable aescalation of privilege through local access.
- CVE-2021-33123—Improper access control in the BIOS authenticated code module for some Intel® Processors may allow a privileged user to potentially enable aescalation of privilege through local access.
- CVE-2021-33124—Out-of-bounds write in the BIOS authenticated code module for some Intel® Processors may allow a privileged user to potentially enable aescalation of privilege through local access.
- CVE-2022-21131—Improper access control for some Intel® Xeon® Processors may allow an authenticated user to potentially enable information disclosure through local access.
- CVE-2022-21136—Improper input validation for some Intel® Xeon® Processors may allow a privileged user to potentially enable denial of service through local access.

Defect ID—CSCwb67157

Cisco UCS B260 M4 Blade Server, Cisco UCS B460 M4 Blade Server, and Cisco UCS C460 M4 Rack Server includes an Intel CPU that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID(s):

- CVE-2021-0154—Improper input validation in the BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable escalation of privilege through local access.
- CVE-2021-0155—Unchecked return value in the BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable information disclosure through local access.
- CVE-2021-0189—Use of out-of-range pointer offset in the BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable aescalation of privilege through local access.

- CVE-2021-33123—Improper access control in the BIOS authenticated code module for some Intel® Processors may allow a privileged user to potentially enable aescalation of privilege through local access.
- CVE-2021-33124—Out-of-bounds write in the BIOS authenticated code module for some Intel® Processors may allow a privileged user to potentially enable aescalation of privilege through local access.

Defect ID—CSCvy67497

Cisco UCS 6400 series FIs include third-party Software that are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2018-14567—If lzma is used with libxml2 2.9.8, it allows remote attackers to cause a denial of service (infinite loop) through a crafted XML file that triggers LZMA_MEMLIMIT_ERROR, as demonstrated by xmllint, a different vulnerability than CVE-2015-8035 and CVE-2018-9251.
- CVE-2018-9251—If lzma is used with the **xz_decomp** function in **xzlib.c** in libxml2 2.9.8, then it allows remote attackers to cause a denial of service (infinite loop) through a crafted XML file that triggers LZMA_MEMLIMIT_ERROR, as demonstrated by xmllint, a different vulnerability than CVE-2015-8035.
- CVE-2021-3541—A flaw was found in libxml2. Exponential entity expansion attack its possible bypassing all existing protection mechanisms and leading to denial of service.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability.

CSCwb59981

Cisco UCS M5 Servers include third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2021-22600—A double free bug in packet_set_ring() in net/packet/af_packet.c can be exploited by a local user through crafted syscalls to escalate privileges or deny service. We recommend upgrading kernel past the effected versions or rebuilding past ec6af094ea28f0f2dda1a6a33b14cd57e36a9755.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability.

CSCvm84140

Cisco UCS Manager is updated with new secure code best practices to enhance the security posture and resilience.

CSCvt82214

Cisco UCS 6400 series FIs include third-party Software that are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2017-15906—The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.
- CVE-2018-15919—Remotely observable behavior in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use.
- CVE-2019-6111—An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp

client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).

Cisco has released software updates that address these vulnerability.

CSCvu63738

Cisco UCS 6400 series FIs include third-party Software that are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2018-15473—OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.
- CVE-2018-15919—Remotely observable behavior in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use.
- CVE-2019-6111—An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).

CSCwa65691

Cisco UCS 6400 series FIs include third-party Software that are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2017-15906—The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.
- CVE-2018-15919—Remotely observable behavior in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use.
- CVE-2019-6111—An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).

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 Firmware Release 4.2(3j)

The following caveats are resolved in Release 4.2(3j):

Defect ID	Symptom	First Bundle Affected
CSCwh04150	On Cisco UCSX-210C compute node with UCSX-I-9108-25G running on version 4.2(2d), packets aimed at IP addresses ending in '136.204' failed to reach the Fabric Interconnect (FI) and not appeared in Embedded Logic Analyzer (ELAM).	4.2(2d)A
CSCwh67130	Upstream network communication problems observed on a setup equipped with Cisco UCS X-Series servers connected to Cisco UCS 9108 25G IFMs.	4.2(1i)A

Resolved Caveats in X-Series M7 Firmware Release 5.1(0.230122)

The following table lists the resolved caveats in X-Series M7 firmware release 5.1(0.230122)

Defect ID	Description	First Bundle Affected
CSCwe52335	Failure accessing the libcipmi SDR information. fcgi-workers0_core.2823 gets generated on server decommission/recommission .	5.1(0.230096)
CSCwe54136	Running HSU causes powercap setting to fail intermittently and requires power cycle of the host to resync the cap limit.	5.1(0.230096)
CSCwe54208	Need to recreate Inband2 with a different VLAN then remove it prior to adding Inband1.	5.1(0.230096)
CSCwe50974	X210c M7 server failed to run profile even though sufficient profile budget was assigned in the Chassis.	5.1(0.230096)
CSCwe47118	Redfish monitor core occured during combinational stress(Redfish stress included).	5.1(0.230096)
CSCwe46276	On M7, boot to the OS, make sure SOL is working fine, after that, reboot BMC, wait till BMC up, the SOL does not work ,need to reboot the host OS to recover it.	5.1(0.230096)
CSCwe65074	Update Device Connector to 1.0.11.2759.	5.1(0.230096)
CSCwe69788	Thermal Trip is observed on rebooting BMC. Processor P1_THERMTRIP #0x53 | Limit Exceeded"	5.1(0.230096)

Defect ID	Description	First Bundle Affected
CSCwe36415	Do not show the Task ID under UpdateService/SoftwareInventory/HSU URL. /redfish/v1/UpdateService/SoftwareInventory/HSU URL, shows the related task ID in "RelatedItem" parameter. At times, after we do factory reset, or when the number of tasks reach to the maximum value, that may delete the related task ID. Checking the displayed task ID in such a case shows 'Critical' error, because the task ID does not exist. Schema validation also fails.	5.1(0.230096)
CSCwe47304	Default gateway does not get set according to a precedence that follows Inband2 > Inband1 > OutbandB > OutbandA.	5.1(0.230096)

Resolved Caveats in X-Series M6 Firmware Release 5.1(0.230075)

The following table lists the resolved caveats in X-Series M6 firmware release 5.1(0.230075)

Defect ID	Description	First Bundle Affected
CSCwe65074	Update Device Connector to 1.0.11.2759.	5.1(0.230054)
CSCwe54208	Need to recreate Inband2 with a different VLAN then remove it prior to adding Inband1.	5.1(0.230054)
CSCwe47304	Default gateway does not get set according to a precedence that follows Inband2 > Inband1 > OutbandB > OutbandA.	5.1(0.230054)
CSCwe84278	Add a proper timeout value for UCSX-V4-Q25GME-RETIMER	5.1(0.230054)

Resolved Caveats in X-Series Firmware Release 5.1(0.230054)

The following table lists the resolved caveats in X-Series firmware release 5.1(0.230054)

Defect ID	Description	First Bundle Affected
CSCvz93600	Add PCH and Q71 sensors in IPMI tool and sensor history log.	5.0(4b)
CSCwc07335	When USB low power is set via jolt_util API or Redfish, the value is not communicated to the KVM.	5.0(2e)
CSCwd04607	Enable Redfish for Inband support in X-Series products.	5.0(4b)
CSCwd07888	Profile deploy is failing on one of X210c Compute Node during deployment of Access policy. Message seen:-"Update in progress, request rejected".	5.0(2b)
CSCwd63892	X210c Compute Nodes blades are in loop for 3 times during BIOS POST with every reset.	5.0(1b)
CSCwd68222	Provide API support so that Redfish support can be enabled for IPMI encryption key.	5.0(4b)
CSCwe10891	Update Device Connector to 1.0.11.2611.	5.0(4b)

Defect ID	Description	First Bundle Affected
CSCwe25043	On a X210c M6 Compute Node, running CIMC 5.1(0.230031), deploy server profile with valid IMC access policy. CIMC will keep the setting in config files jolt_network.json and inband_intf. Now activate the old CIMC 5.0(4a), Intersight shows the Inband IP is configured, however the Inband IP is not accessible.	5.0(4a)
CSCwd91329	Unable to read UCSX-440P PCIe Node GPU temperature via SMBus direct spam after disabling the riser. GPUs get initially fully discovered on UCSX-440P (paired with X210c M6 Compute Node), a host power off/cycle is done directly (within ~5 seconds) after BIOS POST completion. PciNodeUnknownPCieCardPresentOnRiser fault gets raised (UnknownPCIeCardPresentOnRiser[1|2]) which eventually causes Riser[1|2]PowerDisabled (after the next host power off is detected), ultimately causing the IMM GraphicsCardTemperatureCritical fault and I2C temperature spam in BMC ENG syslog.	5.0(4b)

Resolved Caveats in X-Series Firmware Release 5.0(4g) — None

Resolved Caveats in X-Series M7 and M6 Firmware Release 5.0(4f) — None

Resolved Caveats in Release 5.0(4b)

The following table lists the resolved caveats in release 5.0(4b)

Defect ID	Description	First Bundle Affected
CSCwd87584	Support for Oracle Linux OS added for all M6 server.	5.0(1c)
CSCwd88272	IPv naming should be common across all network boots.	5.0(1c)
CSCwe16597	Integrate Intel XL710-QDA2 Dual Port 40Gb adapter firmware.	5.0(1c)
CSCwc48870	Enable secure erase features for UCSX-V4-Q25GML and UCSX-ML-V5D200G adapters.	5.0(1c)
CSCwd66132	Improve tech support collection for UCSX-ML-V5D200G adapters by enabling firmware to collect classifier information such as RDMA data.	5.0(1c)

Resolved Caveats in Release 5.0(4a)

The following table lists the resolved caveats in release 5.0(4a)

Defect ID	Description	First Bundle Affected
CSCwd73568	Transient PciNodePower Fault could appear on UCSX-440P PCIe node in IMM after either of these conditions: • A short chassis power cycle of less than five seconds.(BMC on paired compute node will likely report HSC Fault on UCSX-440P in this case) • The UCSX-210C-M6 compute node is AC power cycled (slot reset) or physically removed/re-inserted while the UCSX-440P PCIe node is still installed in the paired slot. (BMC on paired compute node will likely report DCBrick Fault on UCSX-440P in this case)	5.0(2b)
CSCwa04467	Board controller in UCSX-210C-M6 compute node needs to support UCD firmware update and configuration.	5.0(2e)
CSCwc27394	Add the latest Device Connector (DC) 1.0.9-2159 in 5.0(4a) build.	5.0(2a)
CSCwc45638	Update UCSX-210C-M6 Board Controller to 18.0. The update is required for the following: • UCD update for 3.3v to 3.4v to fix the M.2 issue observed on UCSX-210C-M6 compute node. • UCD change to add the P54V UV fault as a trigger to fail_pwr_seq. Currently when P54V UV fault occurs, the HSC triggers its FAULT GPIO. • INF VR image update to address VR HOT issue. • i2c transactions are failing for board update 17.0	5.0(2a)

Resolved Caveats in Release 5.0(2e)

The following table lists the resolved caveats in release 5.0(2e)

Defect ID	Description	First Bundle Affected
CSCvx55355	AMI Label update for C220 and C240 M6 servers.	5.0(2d)
CSCwc80156	User selects Intel SGX Enable option in BIOS setup menu, boots to Windows, and runs Intel SGX BIOS Info Tool. It is observed that Intel SGX does not get enabled as uCode appears invalid for SGX enabled MCHECK error code = 0x00004811 in M6 servers.	5.0(2d)
CSCwc91429	Update Device Connector to 1.0.11-2209 for M5 and M6 servers.	5.0(1b)
CSCwb09233	Add HSC Temp(Q71) and PCH Temperature sensors to CPWM fan speed control for X210c server.	5.0(1b)
CSCvx54489	Intersight no longer supports the VideoEncryption property. Remove KVM configuration for video encryption on all platforms.	5.0(1b)

Defect ID	Description	First Bundle Affected
CSCwb37591	Add "InvalidFanPolicies" property to CPWM fan control to balance the fan policies when 256 GB DIMMs are present in the blade.	5.0(1c)
CSCwb79633	Remove IPMI thresholds from HSC, PCH, MLOM, and MLOM DIE Temperature sensors. Add these sensors to CPWM fan speed control for X210c servers.	5.0(1b)
CSCwc08368	Expected alarm is not raised in CIMC when XFM2 is removed. User sees a missing health alarm on the GUI for UCSX-GPU-T4-16, UCSX-GPU-A40, UCSX-GPU-A100-80, UCSX-GPU-A16 Graphics Processing Units on UCS X440P.	5.0(2b)
CSCwb90464	Storage is not seen in the Inventory after claiming and discovering x210c server.	5.0(2d)

Resolved Caveats in Release 5.0(2d)

The following table lists the resolved caveats in release 5.0(2d)

Defect ID	Description	First Bundle Affected
CSCwb96614	Self-encrypting drive (SED) status appears unconfigured after reboot. The Storage Firmware package (52.20.0-4523) integrated with 5.0(2d) will fix this issue.	5.0(2b)
CSCwc62657	Cisco UCS X210c M6 servers running BIOS versions 5.0.1h.0, 5.0.1i.0, or 5.0.2c.0 display multiple uncorrectable errors after multiple Memory ECC errors and ADDDC/PCL event when PPR is completed on next reboot.	5.0(1e)

Resolved Caveats in Release 5.0(2b)

The following table lists the resolved caveats in release 5.0(2b)

Defect ID	Description	First Bundle Affected
CSCvw35916	In Cisco UCS X210c M6 servers, the reboot of BMC is not clean. During the reboot, the Network Time Protocol daemon (ntpd) gets started twice and fails the second time.	5.0(1b)
CSCvy52485	Change the Sensor History Logs so that only the highest temperature for a day gets recorded.	5.0(1a)

Defect ID	Description	First Bundle Affected
CSCvz14883	The Syslog shows: *Secure-Action-monitor:1108: 97:uem_connect_to_server:Error connecting to server* *Secure-Action-monitor:1108: src/monitor.c:1528:Security-Check: failed to post event* Secure action monitor is unable to connect and publish event to UEMd. Secure action starts early in boot process and tries to post fault before rest of the infrastructure is up.	5.0(1b)
CSCvz16428	LastPowerState is not set to the power state of the board, when power restore policy is set to LastState.	5.0(1b)
CSCvz55930	After decommissioning or recommissioning of the UCSX-210C-M6 servers, the profile value resets to default (350/1300). All blade servers have valid profile value (minimum/maximum) and must remain unchanged as part of hardware configuration.	5.0(1b)
CSCvz88277	In blade servers, the power profile times out and the Power-State shows *Off* when the boot time exceeds more than ten minutes due to Error correction code (ECC).	5.0(1b)
CSCvz96056	For X-Series servers, Cisco IMC requires an interface to allow the Intersight Managed Mode (IMM) to push a new Product ID Catalog and restart services after the Catalog update. This can be specifically used for Drive, Memory, or CPU, as they do not require a full image verification.	5.0(1b)
CSCwa67582	Add Temperature sensor to Fan Control for monitoring and maintaining the health of Virtual Interface Card (*VIC*) and LAN-on-motherboard (*mLOM*) adapter.	5.0(1b)
CSCwa88344	The Device Connector (DC) upgrade fails due to syntax error (line 136 and line 140) in *update-utility.sh*. Update to find the correct version line for DC image during an update.	5.0(1b)
CSCwb23534	For UCSBX-9508, change the slots of UCSX-V4-PCIME and UCSX-V4-Q25GME initially reported as REAR-MEZZ to PCI-MEZZ-XFABRIC (PCI-MEZZ1-XFABRIC and PCI-MEZZ2-XFABRIC).	5.0(1c)
CSCwb85297	The Device Connector (DC) restarts multiple times, shows *fatal error: concurrent map writes*. Add the latest Device Connector (DC) 1.0.9-2021 in 5.0(2b) build.	5.0(1e)
CSCwc03295	In the Cisco UCS X210c M6 servers, Cisco Integrated Management Controller (CIMC) libpeci is not handling 0x94 CC during crashdump collection. Disable UMA timeout in BIOS and consider PECI CC 0x94 as successful completion to resolve this issue.	5.0(1c)

Resolved Caveats in Release 5.0(1f)

The following table lists the resolved caveats in release 5.0(1f)

Defect ID	Description	First Bundle Affected
CSCwb96971	In UCSX-210C-M6 servers, M.2 drives fail randomly resulting in degraded Virtual Disks.	5.0(1e)

Resolved Caveats in Release 5.0(1e)

The following table lists the resolved caveats in release 5.0(1e)

Defect ID	Description	First Bundle Affected
CSCwb09802	BIOS token should carry Server Profile, Template, and System Information so that the same can be retrieved from Host Operating System (OS).	5.0(1b)
CSCvx95585	System Management BIOS Type 11 has missing parameters: $SPI, $SPT, $SYS.	5.0(1b)
CSCwb21466	Add Kioxia PM6-ISE SSD firmware 0103 into B200 M6 server in Intersight Managed Mode.	5.0(1c)
CSCwb21467	Add Kioxia PM6-FIPS SSD firmware 0103 into B200 M6 server in Intersight Managed Mode.	5.0(1c)
CSCwa98937	The description message for Storage Firmware Downgrade from 5.1 Pkg 52.20.0-4432 to 5.0(1b) Pkg 52.15.0-3988 needs to be modified.	5.0(1b)
CSCwa22730	Fix the description message for Storage controller UCSX-X10C-RAIDF SPDM failure issue.	5.0(1b)
CSCwb88505, CSCwb81096	Fix for the discovery core during Host Service Utility (HSU) inventory of 5.0(1c).	5.0(1c)
CSCwb28440	Few Cisco UCS X210c Blade servers fail to start the Device Connector (DC). It results in the DC mount failure on the server, thereby causing all the server discoveries to fail.	5.0(1b)

Resolved Caveats in Release 5.0(1c)

The following table lists the resolved caveats in Release 5.0(1c):

Defect ID	Description	First Bundle Affected
CSCvz19856	The Intel® Intelligent Power Technology Node Manager (NM) PTU intermittently fails to run on Cisco UCSX-210C-M6 server during boot up interrupting the Power profile execution	5.0(1b)

Defect ID	Description	First Bundle Affected
CSCvz25126	The measurements on the input power reading on the Cisco UCSX-210C-M6 server and the output power reading in the main Hot-swap controller are different.	5.0(1b)
CSCvz69262	When enabling STEP in BIOS policy, the check BiosTech.log and find memory test did not work on the following DIMMs and this issue is resolved. • UCS-ML-128G4RW • UCS-MR-X64G2RW • UCS-MR-X32G1RW • UCS-MR-X16G1RW • UCS-ML-128G4RW • UCS-MR-X64G2RW • UCS-MR-X32G1RW • UCS-MR-X16G1RW	5.0(1b)
CSCwa10354	In the Cisco UCSX-210C-M6 server, the Node Manager cannot access the Power Cap configured files resulting in intermittent power profiling failure or profile data loss.	5.0(1b)
CSCwa15349	The default behavior for M6 systems is to enforce DIMM population (POR). After a DIMM failure, this enforcement disables a considerable amount of memory and flags the additional DIMMs as Invalid Population.	5.0(1b)
CSCwa16535	Added support for enhancing CPU Performance Token UCSX-210C-M6 to adjust Voltage Regulator (VR) setting, allowing it to increase processor performance.	5.0(1b)

Resolved Caveats in C-Series Server Firmware

Resolved Caveats in Release 4.3(3m)

The following caveats are resolved in Release 4.2(3m):

Defect ID	Description	First Bundle Affected
CSCwm02322	In Cisco UCS C220 M5 servers, the XML API commands for fault monitoring does not capture the fan alerts.	4.1(3c)

Resolved Caveats in C-Series M5 and M6 Firmware Release 4.2(3l)

The following caveats are resolved in Release 4.2(3l):

Defect ID	Description	First Bundle Affected
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 M7 and M6 Firmware Release 4.2(3j) — None

Resolved Caveats in Release 4.2(3i)

The following caveats are resolved in Release 4.2(3i):

Defect ID	Symptom	First Bundle Affected
CSCwb82433	Cisco UCS C220 M5 servers equipped with Cisco UCS VIC 1400 series adapter and have *Geneve* enabled, go offline after the Cisco UCS VIC adapters fail to respond.	4.2(2a)
CSCwf88211	Cisco UCS C240 M6 servers shows the following error while in operation: `AdapterHostEthInterfaceDown` There is no functionality impact on the server.	4.2(3h)

Resolved Caveats in C-Series Firmware Release 4.2(3h)

The following caveats are resolved in Release 4.2(3h):

Defect ID	Symptom	First Bundle Affected
CSCwe92151	When some specific model of HDDs are inserted or the drives are initialized during any operation in a Cisco UCS C-series M6 or M7 server, the server automatically powers ON from OFF state. This results low level firmware update failure.	4.3.2.230207

Resolved Caveats in C-Series Firmware Release 4.2(3g)

The following table lists the resolved caveats in C-Series firmware release 4.2(3g)

Defect ID	Description	First Bundle Affected
CSCwe61589	In Cisco UCS C220 M5 servers, Intelligent Platform Management Interface (IPMI) goes into a constant restart loop after application stall messages, causing IPMI management to fail.	4.1(3c)

Defect ID	Description	First Bundle Affected
CSCwd46043	During regular operation of the Cisco UCS C240 M5 server, Cisco IMC might lose management plane connectivity. There might not be impact on the data plane as the Cisco IMC (management plane) is the affected component and the connectivity is restored on its own.	4.2(2a)

Resolved Caveats in Release 4.2(3b)

The following table lists the resolved caveats in C-Series firmware release 4.2(3b)

Defect ID	Description	First Bundle Affected
CSCwd79791	Missing hypen in json file of ucs-c245m6-hx-Catalog.json.	4.2(2g)
CSCwd68472	Server firmware upgrade failed at "Wait for firmware upgrade to complete.The operation has timed out."	4.2(2g)

Resolved Caveats in Release 4.2(2g)

The following table lists the resolved caveats in C-Series firmware release 4.2(2g)

Defect ID	Description	First Bundle Affected
CSCwd56630	Unexpected Host Power Cycle is observed when NIHUU Update is in Progress for C480 M5 server.	4.2(2f)
CSCwc76592	M6 Expansion fails as the SAS controller disappears. On trying to expand a 2N 5.0.2a M5 Edge cluster with 2 M6 converge nodes, the expansion is failing at "Configure Hypervisor Management Network". SAS Controller has disappeared in the CIMC. The expansion failure is seen on both the M6 servers.	4.2(2b)
CSCwd03250	DST Feature Incorrectly Marks Global Hot Spare as Bad. On 4.2(2a) firmware, you may encounter "Local disk X is degraded" faults. This may happen every 7 days.	4.2(2a)
CSCwb01975	Intel ADP-RR NVMe drive has FRU VPD data missing. Few fields are missing from FRU VPD - capacity (nvme_vpd_mra), Manufacturer name, Product Name, Product Part Number/Model, Product version, Product Serial Number.	4.2(1a)
CSCwd29230	Remove UCS-NVMEHY-W3200 and UCS-NVMEHY-W1600 LFF PID for M6 platforms.	4.2(2f)

Defect ID	Description	First Bundle Affected
CSCwc10747	VIC FLS process may crash when unexpected order of events occur during SAN boot. In very rare circumstance where sequence of events in SAN boot do not occur as expected, FLS process may crash on VIC adapter, showing the following in VIC OBFL after an ASSERT error: (/bin/fls) exited due to receiving signal 11 - Segmentation fault (core dumped)	4.2(2f)
CSCwd33432	Server profile association failed on C220-M5L server at unconfigAllNic failed for UCSC-MLOM-C100-04 and UCSC-PCIE-C100-04 adapters.	4.2(2f)

Resolved Caveats in Release 4.2(2b)

The following table lists the resolved caveats in C-Series firmware release 4.2(2b)

Defect ID	Description	First Bundle Affected
CSCwc34359	Add SAN drives details to the logs directory. Copy SAN drives details from /sys/firmware/ibft , /sys/class/fc_host and /sys/class/fc_transport directories to the logs directory and this info should be reflected in tech-support file.	4.2(2a)
CSCwc38237	Update scu source code with megaraid_sas driver (RHEL8.2 , RHEL7.9)	4.2(2a)
CSCwc27924	Reduce the size of the SDU iso to fit into flex util partition as there is a size restriction 256 MB.	4.2(2a)
CSCwc26997	Upgrading the server from 4.2(1b) to 4.2(1f) failed on HDD model MTFDDAK120TDT.	4.2(1b)

Resolved Caveats in Release 4.2(1j)

The following table lists the resolved caveats in C-Series firmware release 4.2(1j)

Defect ID	Description	First Bundle Affected
CSCwb69579	Individual component firmware update fails for Intel i350 Quad Port 1Gb Adapter. Update was triggered for Intel i350 Quad Port 1Gb Adapter. Task ID response was verified. The update fails with "Cannot boot to HSU OS" error.	4.2(1i)
CSCwc23748	During an HSU Downgrade from 4.2 to 4.1, HSU Update task got stuck for long time and then an Exception:Cannot boot HSU OS was seen.	4.2(1i)
CSCvx55355	AMI Label merges for C220 and C240 M6 servers.	4.2(1i)

Defect ID	Description	First Bundle Affected
CSCwa56128	All Intel cards is failing while downgrading firmware. Downgrade firmware from ucs-c240m6-huu-4.2.1.144.iso to ucs-c240m6-huu-4.2.1e.211202.iso. Select all components and trigger for update. Firmware update failed for X550 card.	4.2(1i)
CSCwc37184	RHEL OS is going to emergency mode after updating BIOS from CIMC. This is observed on latest BIOS C220M6.4.2.1i.6.0703222157.	4.2(1i)
CSCwc18223	Some SED drives are being set to unconfigured good on reboot when secure UEFI is enabled, forcing a rebuild of the RAID.	4.2(1f)
CSCwb83355	VIC will report firmware/scsi status as DATA_CNT_MISMATCH/RESERVATION_CONFLICT if the target does not set RESID bits for any IO that receives RESERVATION_CONFLICT status. ESX SCSI layer will consider DATA_CNT_MISMATCH as a failure and ignore the RESERVATION_CONFLICT SCSI status. If too many reservation conflict are received, it may degrade the Virtual Machines performances.	4.2(1i)

Resolved Caveats in Release 4.2(1g)

The following table lists the resolved caveats in C-Series firmware release 4.2(1g)

Defect ID	Description	First Bundle Affected
CSCwa98283	The upgrade on the endpoint is stuck in NIHUU upgrade where the host continuously reboots and tries to mount the new image and asks for EULA. This is observed while upgrading C220 M5 servers with locally mounted vmedia of HUU.	4.1(3c)
CSCwb04635	While updating the C225 and C245 M6 servers firmware components from 4.2(1f) to 4.2(1g), failure is observed at BIOS update/activation.	4.2(1f)
CSCwb07978	Sensor reading and GPU inventory fails to detect for Nvidia A16 GPU. C245 M6 server is upgraded with latest BIOS and CIMC firmware, A16 GPU is connected and latest HUU is attached. After logging to CIMC, it is observed on GPU Inventory page that A16 details are not listed.	4.2(1f)

Resolved Caveats in Release 4.2(1f)

The following table lists the resolved caveats in C-Series firmware release 4.2(1f)

Defect ID	Description	First Bundle Affected
CSCvz89363	After downgrading IT controller Firmware from 20.65.05.00 to 16.65.28.00 on C225 and C245 M6 servers, Out-of-Band mode is changing from I2c to PCIe and the controller is not getting discovered in CIMC.	4.2(1e)
CSCvz77885	An unknown reboot of CIMC was reported during normal operation of the Cisco UCS C240 M5 server. This is reported for CIMC version 4.1(3d).	4.2(1e)
CSCwa22529	Bios firmware update status is not getting updated automatically for Bios Activation. This is observed for C 225 and C245 M6 servers with CIMC build 4.2(1d) and Bios Ver C245M6.4.2.1c.0.080621134.	4.2(1e)

Resolved Caveats in B-Series Server Firmware

Resolved Caveats in B-Series M6 Firmware Release 5.1(0.230069)

The following table lists the resolved caveats in B-Series M6 firmware release 5.1(0.230069)

Defect ID	Description	First Bundle Affected
CSCwe47304	Default gateway does not get set according to a precedence that follows Inband2 > Inband1 > OutbandB > OutbandA.	5.1(0.230052)
CSCwe65074	Update Device Connector to 1.0.11.2759.	5.1(0.230052)
CSCwe54208	Need to recreate Inband2 with a different VLAN then remove it prior to adding Inband1.	5.1(0.230052)

Resolved Caveats in B-Series M5 Firmware Release 5.1(0.230073)

The following table lists the resolved caveats in B-Series M5 firmware release 5.1(0.230073)

Defect ID	Description	First Bundle Affected
CSCwe65074	Update Device Connector to 1.0.11.2759.	5.1(0.230054)
CSCwe54208	Need to recreate Inband2 with a different VLAN then remove it prior to adding Inband1.	5.1(0.230054)
CSCwe47304	Default gateway does not get set according to a precedence that follows Inband2 > Inband1 > OutbandB > OutbandA.	5.1(0.230054)

Resolved Caveats in B-Series Firmware Release 5.1(0.230052)

The following table lists the resolved caveats in B-Series firmware release 5.1(0.230052).

Defect ID	Description	First Bundle Affected
CSCwa47736	KVM client top right menus do not work on resizing the browser window. This is observed on Firefox browser.	4.2(3b)
CSCwb87775	Kernel panic is observed and CIMC reboots on doing discovery stress for B-Series M6 servers.	4.2(2e)
CSCwd17871	The IPMI commands using the Inband IPv4 IPs of the B-Series M6 server is not working while the same is working with OOB IPs.	4.2(3b)
CSCwd04607	Enable Redfish for Inband support in B-series products.	4.2(3b)
CSCwe10891	Update Device Connector to 1.0.11.2611.	4.2(3b)

Resolved Caveats in B-Series Firmware Release 5.1(0.230054)

The following table lists the resolved caveats in B-Series M5 firmware release 5.1(0.230054).

Defect ID	Description	First Bundle Affected
CSCwb87775	Kernel panic is observed and CIMC reboots on doing discovery stress for B-Series M5 servers.	4.2(2e)
CSCwd17871	The IPMI commands using the Inband IPv4 IPs of the B-Series M5 server is not working while the same is working with OOB IPs.	4.2(3b)
CSCwd04607	Enable Redfish for Inband support in B-series products.	4.2(3b)
CSCwe10891	Update Device Connector to 1.0.11.2611.	4.2(3b)
CSCvs49681	When one OOB interface is removed, it clears out the gateway in the other OOB interface even though it has not been explicitly removed. The other gateway will still have address, netmask, hostname, VLAN.	4.2(3b)

Resolved Caveats in B-Series Firmware Release 4.2(3j) — None

Resolved Caveats in B-Series Firmware Release 4.2(3i) — None

Resolved Caveats in B-Series Firmware Release 4.2(2e)

The following table lists the resolved caveats in B-Series firmware release 4.2(2e)

Defect ID	Description	First Bundle Affected
CSCwd29415	Add RHEL 8.7 and RHEL9.1 OS Support to SCU DB.	4.2(2d)
CSCwd29230	Remove UCS-NVMEHY-W3200 and UCS-NVMEHY-W1600 LFF PID for B-Series M6 servers.	4.2(2d)
CSCwa79931	Include temperature monitoring and fan control of MLOM temps to UCSX-I-9108-100G Chassis for UCSB-ML-V5Q10G mLOM.	4.2(2d)

Resolved Caveats in B-Series Firmware Release 4.2(2b)

The following table lists the resolved caveats in B-Series firmware release 4.2(2b)

Defect ID	Description	First Bundle Affected
CSCwc38237	Update scu source code with megaraid_sas driver (RHEL8.2 , RHEL7.9).	4.2(2a)

Resolved Caveats in B-Series Firmware Release 4.2(1h)

The following table lists the resolved caveats in B-Series firmware release 4.2(1h)

Defect ID	Description	First Bundle Affected
CSCwc27394	Update B200 M6 firmware images to DC 1.0.9-2159.	4.2(1f)
CSCwc03295	libpeci not handling 0x94 CC during crashdump collection. This impacts crashdump collection on all platforms resulting in crashdump output json file that contains invalid (garbage) data that is not useful in aiding system debug in the event of CATERR.	4.2(1f)

Resolved Caveats in B-Series Firmware Release 4.2(1f)

The following table lists the resolved caveats in B-Series firmware release 4.2(1f)

Defect ID	Description	First Bundle Affected
CSCvx95585	Smbios type 11 missing $SPI,$SPT and $SYS for B200 M6 server.	4.2(1e)
CSCwa33158	The UCS-B200-M6 server power consumption reading is found to be 9% less than the actual power the server consumes.	4.2(1e)
CSCwa85667	BMC reset observed on M5 and M6 servers due to kernel crash and watchdog reset. This normally triggers shallow discovery.	4.1(3b)
CSCvx37634	Blade discovery will fail and generate a fault in UCSM stating: "Setup of Vmedia failed(sam:dme:ComputeBladeDiscover:SetupVm	4.1(3b)

Resolved Caveats in B-Series Firmware Release 4.2(1c)

The following table lists the resolved caveats in B-Series firmware release 4.2(1c)

Defect ID	Description	First Bundle Affected
CSCvz29291	HTTP or HTTPS mounted vMedia may not work with certain hosting tools. When attempting to mount an ISO to a server using the Cisco APIs through HTTP or HTTPS, the server will correctly show the volume and remote share details. It will work on this and ultimately fail with the error: "Local Device Mount Failed" in the status column.	4.1(3b)
CSCvz46580	KVM Login with OTP credentials shows "Login denied".	4.1(3b)

Defect ID	Description	First Bundle Affected
CSCvy88260	For B480M5 server with UCSB-MRAID12G-HE 4x SATA physical drives, the "Model" info is missing.	4.1(3b)

Open Caveats

Open Caveats in X-Series 5.0(4g), C-Series 4.2(3m), and B-Series 4.2(3j) Firmware — None

Open Caveats in X-Series 5.0(4f), C-Series 4.2(3l), and B-Series 4.2(3i) Firmware — None

Open Caveats in C-Series Firmware Release 4.2(3j) — None

Open Caveats in X-Series Firmware Release 5.0(2b)

The following caveats are open in X-Series firmware Release 5.0(2b):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwb96316	In Cisco UCS X210c M6 servers, MRAID controller and disks do not get detected in the inventory after firmware upgrade to 5.0(2b) from 5.0(1c) or 5.0(1e).	Rerun the firmware upgrade from Intersight Managed Mode.	5.0(1c)

Open Caveats in X-Series Firmware Release 5.0(1f)

The following caveats are open in X-Series firmware release 5.0(1f):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwb96316	In Cisco UCS x210c M6 servers, MRAID controllers are disappearing from the inventory after firmware upgrade to 5.0(1f) from 5.0(1c) and 5.0 (1e).	Rerun the firmware upgrade from Intersight Managed Mode.	5.0(1c)

Known Limitations and Behavior

VR settings to be adjusted to enable CPU Performance Enhancement

CSCwa15491 - The VR setting has to be adjusted to enable CPU Performance Enhancement setting in BIOS for UCSX-210C-M6 servers.