

Release Notes for Cisco Intersight Managed Mode Server Firmware, Release 6.0

First Published: 2025-08-05

Last Modified: 2026-10-26

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

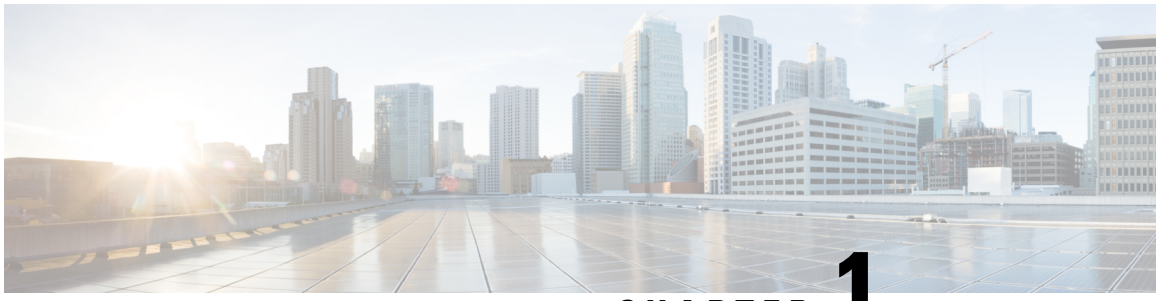
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2025–2026 Cisco Systems, Inc. All rights reserved.



CHAPTER 1

Cisco Intersight Managed Mode Server Firmware, Release 6.0

- Cisco Intersight Managed Mode Server Firmware, Release 6.0, on page 1
- Firmware Version Equivalency Between Cisco Intersight, Cisco IMC, and Cisco UCS Manager, on page 2
- Latest supported firmware for end-of-life Intersight Managed Mode servers, on page 2
- Revision History, on page 3

Cisco Intersight Managed Mode Server Firmware, Release 6.0

Cisco Intersight Managed Mode server firmware updates are released to provide updated versions of BIOS, CIMC, adapters, and other server components for supported Cisco UCS servers and Cisco Unified Edge servers managed through Intersight. To manage the server firmware, Cisco UCS server firmware, see Managing Firmware in Intersight Managed Mode and Upgrading Firmware for Unified Edge Compute Nodes. This feature is available with a Cisco Intersight Essentials or Advanced license tier.

Note This document covers known issues and limitations related to these IMM servers only.

Supported servers managed through Intersight are:

- **Intersight Managed Mode (IMM) servers:**

  These include:

  - Cisco UCS XE-Series Unified Edge servers connected to Intersight through Edge Chassis Management Controllers (eCMC).
  - Cisco UCS X-Series, B-Series, and C-Series servers connected to Intersight through Cisco UCS Fabric Interconnects (FI).

- **Intersight Standalone Mode servers:**

  These include Cisco UCS C-Series and S-Series rack servers without Fabric Interconnect attachment, managed by Cisco Integrated Management Controller (CIMC). For known issues and limitations related to ISM servers, see Cisco IMC Release Notes.

- **UCS Manager (UCSM) Managed Mode (UMM) servers:**

  These include Cisco UCS B-Series, C-Series, X-Series, S-Series, and HX-Series servers, which are attached to Fabric Interconnects (FIs), and managed through UCS Manager.

  For known issues and limitations related to UMM servers, see Cisco UCS Manager Release Notes.

- **Cisco UCS C885A M8 Rack server:**

  For known issues and limitations related to Cisco UCS C885A M8 Rack server, see Cisco Baseboard Management Controller Release Notes for Cisco UCS C885A M8 Rack Server.

- **Cisco UCS C845A M8 Rack server:**

  For known issues and limitations related to Cisco UCS C845A M8 Rack server, see Cisco Baseboard Management Controller 2.0 Release Notes, Release 2.0.

Firmware upgrades in Intersight include both server and infrastructure firmware updates, which can be updated independently. That is, you do not always need to upgrade the Fabric Interconnects or Unified Edge Chassis Management Controller (eCMC) infrastructure firmware to use the latest server firmware and vice versa. For more information on compatibility between infrastructure firmware and server firmware, see Cross Version Firmware Support. For more information on infrastructure firmware updates, see Release Notes for Cisco Intersight Managed Mode Infrastructure Firmware and Release Notes for Cisco Intersight Unified Edge eCMC Infrastructure Firmware.

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.

To view the complete matrix in PDF format, click here.

Latest supported firmware for end-of-life Intersight Managed Mode servers

Platform	Supported Latest Firmware version
Cisco UCS C-Series M5 (C220, C240, C480)	4.3(2.260020)
Cisco UCS C-Series M6 (C220, C240)	6.0(2.260205)
Cisco UCS B-Series M5 (B200, B480)	6.0(1.260031)
Cisco UCS B-Series M6 (B200)	6.0(2.260205)

For more information, see End-of-Life and End-of-Sale Notices for C-Series Servers and End-of-Life and End-of-Sale Notices for B-Series Servers.

Revision History

The following table includes the change history for this document.

Table 1: Release 6.0.2

Revision Date	Description
October 26, 2026	Updated release notes for Cisco UCS C-Series C220 M8 and C240 M8 Server Firmware Release 6.0(2.260236). This release includes updates to Resolved issues. It does not include any new hardware support, security fixes, or open issues.
October 01, 2026	Added CSCwt77804 under • Security fixes
September 23, 2026	Updated release notes for the following Server Firmware Release versions: • Cisco UCS X-Series M8, M7, and M6 Server Firmware Release 6.0(2.260205) • Cisco UCS C-Series M8, M7, and M6 Server Firmware Release 6.0(2.260205) • Cisco UCS B-Series M6 Server Firmware Release 6.0(2.260205) This release includes updates to: • Resolved issues It does not include any new hardware, security fixes, or open issues.
August 17, 2026	Updated release notes for the following Server Firmware Release versions: • Cisco UCS X-Series M8 and M7 Server Firmware Release 6.0(2.260180) • Cisco UCS C-Series M8 and M7 Server Firmware Release 6.0(2.260180) This release includes updates to: • New hardware It does not include any security fixes, resolved issues, or open issues.

Revision Date	Description
June 25, 2026	Updated release notes for the following Server Firmware Release versions: • Cisco UCS X-Series M8, M7, and M6 Server Firmware Release 6.0(2.260143) • Cisco UCS XE-Series M8 Server Firmware Release 6.0(2.260143) • Cisco UCS C-Series M8, M7, and M6 Server Firmware Release 6.0(2.260143) • Cisco UCS B-Series M6 Server Firmware Release 6.0(2.260143) This release includes updates to: • New hardware • Resolved issues • Open issues It does not include any security fixes.
April 23, 2026	Updated release notes for the following Server Firmware Release versions: • Cisco UCS X-Series M8, M7, and M6 Server Firmware Release 6.0(2.260069) • Cisco UCS C-Series M8, M7, and M6 Server Firmware Release 6.0(2.260069) • Cisco UCS B-Series M6 Server Firmware Release 6.0(2.260069) This release includes updates to: • New hardware • Security fixes • Resolved issues • Open issues

Revision Date	Description
March 16, 2026	Updated release notes for the following Server Firmware Release versions: • Cisco UCS X-Series M8, M7, and M6 Server Firmware Release 6.0(2.260040) • Cisco UCS XE-Series M8 Server Firmware Release 6.0(2.260042) • Cisco UCS C-Series M8, M7, and M6 Server Firmware Release 6.0(2.260044) • Cisco UCS B-Series M6 Server Firmware Release 6.0(2.260040) This release includes updates to: • New hardware • Security fixes • Resolved issues • Open issues • Known issues

Table 2: Release 6.0.1

Revision Date	Description
October 09, 2026	Added CSCwt77804 under • Security fixes
July 14, 2026	Updated release notes for the following Server Firmware Release versions: • Cisco UCS B-Series M5 Server Firmware Release 6.0(1.260031) This release includes updates to: • Resolved issues It does not include any new hardware, security fixes, or open issues.
March 27, 2026	Intersight Infrastructure Firmware version 6.0(1.260006) has been released. There is no corresponding Server Firmware release.

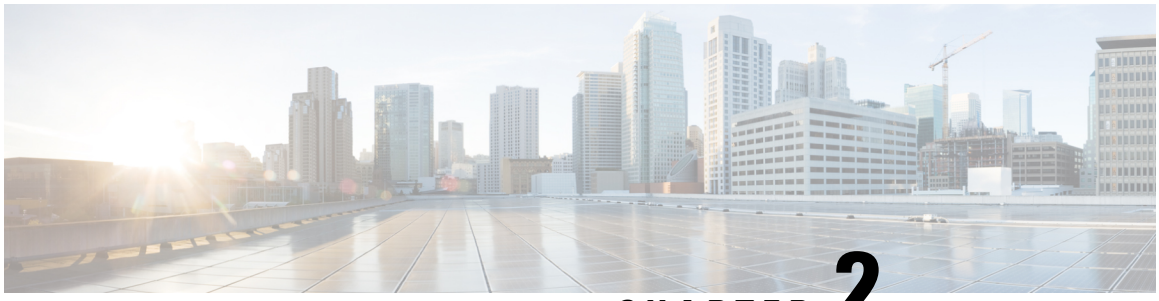
Revision Date	Description
March 16, 2026	Updated release notes for the following Server Firmware Release versions: • Cisco UCS B-Series M5 Server Firmware Release 6.0(1.260012) This release includes updates to: • Resolved issues • Security fixes It does not include any new hardware or open caveats.
February 06, 2026	Intersight Infrastructure Firmware version 6.0(1.260003) has been released. There is no corresponding Server Firmware release.
January 16, 2026	Updated release notes for the following Server Firmware Release versions: • Cisco UCS XE-Series M8 Server Firmware Release 6.0(1.260001) This release includes updates to: • Resolved issues in Cisco UCS XE-Series M8 Server Firmware Release, 6.0(1.260001), on page 56 It does not include any new hardware, security fixes, or open caveats.
January 14, 2026	Updated release notes for Cisco UCS C-Series M8 Server Firmware Release 6.0(1.250194). This release includes a BMC firmware update that addresses a critical power-on issue affecting the Cisco UCS C220 M8. It does not include any new hardware, security fixes, resolved caveats, or open caveats.

Revision Date	Description
December 18, 2025	Updated release notes for the following Server Firmware Release versions: • Cisco UCS X-Series M7 and M6 Server Firmware Release 6.0(1.250179) • Cisco UCS X-Series M8 Server Firmware Release 6.0(1.252114) • Cisco UCS B-Series M6 and M5 Server Firmware Release 6.0(1.250169) • Cisco UCS C-Series M8, M7, and M6 Server Firmware Release 6.0(1.250192) This release includes updates to: • Resolved issues in Cisco UCS X-Series M7 6.0(1.250179) and C-Series M7, M6 6.0(1.250192) Server Firmware Release, on page 56 • Open issues in Cisco UCS X-Series M8 6.0(1.252114) and C-Series M8 6.0(1.250192) Server Firmware Release, on page 68 It does not include any new hardware support or open caveats. Cisco UCS X580p PCIe Node firmware version 6.0(1.252050) and Cisco UCS X9508 Chassis firmware version 6.0(1.252050) have been released.
December 12, 2025	Updated the following sections: • New hardware in Cisco UCS X-Series M8 Server Firmware Release, 6.0(1.252039), on page 20 to include support forCisco UCS X580p PCIe Node and Cisco UCS X9516 X-Fabric.

Revision Date	Description
December 01, 2025	Updated release notes for the following Server Firmware Release versions: • Cisco UCS XE-Series M8 Server Firmware Release 6.0(1.251030) This release includes updates to: • New hardware in Cisco UCS XE-Series M8 Server Firmware Release, 6.0(1.251030), on page 17 • Open issues in Cisco UCS XE-Series M8 Server Firmware Release, 6.0(1.251030), on page 68 • Known issues in Cisco UCS XE-Series M8 Server Firmware Release, 6.0(1.251030), on page 78 It does not include any resolved caveats.
November 21, 2025	Updated release notes for Cisco UCS X-Series M8 Server Firmware Release 6.0(1.252039). It does not include any new hardware, security fixes, resolved caveats, or open caveats.
November 12, 2025	Updated release notes for the following Server Firmware Release versions: • Cisco UCS X-Series M8, M7, and M6 Server Firmware Release 6.0(1.250162) • Cisco UCS B-Series M6 and M5 Server Firmware Release 6.0(1.250157) • Cisco UCS C-Series M8, M7, and M6 Server Firmware Release 6.0(1.250174) This release includes updates to: • Security fixes in Cisco UCS C-Series M8, M7, M6 6.0(1.250174) Server Firmware Release, on page 42 • Resolved issues in Cisco UCS X-Series M8 6.0(1.250162) and C-Series M8, M6 6.0(1.250174) Server Firmware Release, on page 57 It does not include any new hardware or open caveats.

Revision Date	Description
October 09, 2025	Updated release notes for the following Server Firmware Release versions: • Cisco UCS X-Series M8, M7, and M6 Server Firmware Release 6.0(1.250122) • Cisco UCS B-Series M6 and M5 Server Firmware Release 6.0(1.250127) • Cisco UCS C-Series M8, M7, and M6 Server Firmware Release 6.0(1.250131) This release includes updates to: • Resolved issues in Cisco UCS X-Series M8, M7, M6 6.0(1.250122), B-Series M6, M5 6.0(1.250127), and C-Series M8, M7, M6 6.0(1.250131) Server Firmware Release, on page 60 It does not include any new hardware, security fixes, or open caveats.

Revision Date	Description
September 02, 2025	Created release notes for the following Server Firmware Release versions: • Cisco UCS X-Series M8, M7, and M6 Server Firmware Release 6.0(1.250120) • Cisco UCS B-Series M6 and M5 Server Firmware Release 6.0(1.250126) • Cisco UCS C-Series M8, M7, and M6 Server Firmware Release 6.0(1.250127) • Cisco UCS C-Series M8 (6.0(1.250127), 6.0(1.250130)), M7 (6.0(1.250127)), and M6 (6.0(1.250127)) Server Firmware Release This release includes updates to: • New hardware in Cisco UCS X-Series M8, M7, M6 6.0(1.250120) and C-Series M8, M7, M6 6.0(1.250127) Server Firmware Release, on page 21 • Security fixes in Cisco UCS X-Series M8, M7, M6 6.0(1.250120), B-Series M6, M5 6.0(1.250126), and C-Series M8, M7, M6 6.0(1.250127) Server Firmware Release, on page 43 • Resolved issues in Cisco UCS C-Series M8, M7, and M6 6.0(1.250127) Server Firmware Release, on page 60 • Open issues in Cisco UCS X-Series M8, M7, M6 6.0(1.250120), B-Series M6, M5 6.0(1.250126), and C-Series M8, M7, M6 6.0(1.250127) Server Firmware Release, on page 71 • Known issues in Cisco UCS C-Series M8, M7, and M6 6.0(1.250127) Server Firmware Release, on page 79



CHAPTER 2

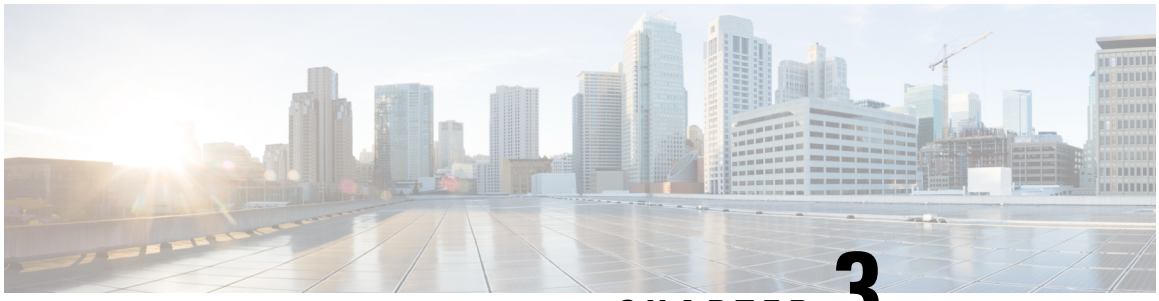
New software features

• New software features, on page 11

New software features

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 software features



CHAPTER 3

New hardware features

- New hardware in Cisco UCS C-Series C220 M8 and C240 M8 6.0(2.260236) Server Firmware Release — None, on page 14
- New hardware in Cisco UCS X-Series M8, M7, M6 6.0(2.260205), C-Series M8, M7, M6 6.0(2.260205), and B-Series M6 6.0(2.260205) Server Firmware Release — None, on page 14
- New hardware in Cisco UCS X-Series M7 6.0(2.260180) and C-Series M7 6.0(2.260180) Server Firmware Release, on page 14
- New hardware in Cisco UCS B-Series M5 6.0(1.260031) Server Firmware Release — None, on page 15
- New hardware in Cisco UCS X-Series M8, M7 6.0(2.260143) and C-Series M8 6.0(2.260143) Server Firmware Release, on page 15
- New hardware in Cisco UCS X-Series M8, M7 6.0(2.260069) and C-Series M8 6.0(2.260069) Server Firmware Release, on page 15
- New hardware in Cisco UCS B-Series M5 6.0(1.260012) Server Firmware Release — None, on page 16
- New hardware in Cisco UCS X-Series M8, M7 Server Firmware Release, 6.0(2.260040), on page 16
- New hardware in Cisco UCS XE-Series M8 Server Firmware Release, 6.0(1.260001) — None, on page 17
- New hardware in Cisco UCS C-Series M8 6.0(1.250194) Server Firmware Release — None, on page 17
- New hardware in Cisco UCS X-Series M8 6.0(1.252114), M7, M6 6.0(1.250179), B-Series M6, M5 6.0(1.250169), and C-Series M8, M7, M6 6.0(1.250192) Server Firmware Release — None, on page 17
- New hardware in Cisco UCS XE-Series M8 Server Firmware Release, 6.0(1.251030), on page 17
- New hardware in Cisco UCS X-Series M8 Server Firmware Release, 6.0(1.252039), on page 20
- New hardware in Cisco UCS X-Series M8, M7, M6 6.0(1.250162), B-Series M6, M5 6.0(1.250157), and C-Series M8, M7, M6 6.0(1.250174) Server Firmware Release — None, on page 21
- New hardware in Cisco UCS X-Series M8, M7, M6 6.0(1.250122), B-Series M6, M5 6.0(1.250127), and C-Series M8, M7, M6 6.0(1.250131) Server Firmware Release — None, on page 21
- New hardware in Cisco UCS X-Series M8, M7, M6 6.0(1.250120) and C-Series M8, M7, M6 6.0(1.250127) Server Firmware Release, on page 21

New hardware in Cisco UCS C-Series C220 M8 and C240 M8 6.0(2.260236) Server Firmware Release — None

New hardware in Cisco UCS X-Series M8, M7, M6 6.0(2.260205), C-Series M8, M7, M6 6.0(2.260205), and B-Series M6 6.0(2.260205) Server Firmware Release — None

New hardware in Cisco UCS X-Series M7 6.0(2.260180) and C-Series M7 6.0(2.260180) Server Firmware Release

- Added support for the following DDR5 Dual Inline Memory Modules (DIMMs), rated for a memory transfer speed of 6400 MT/s on Cisco UCS X215c M8 Compute Node and Cisco UCS C245 M8 and C225 M8 Rack servers:
  - UCS-MRX16G1RE5
  - UCS-MRX32G1RE5
  - UCS-MR128G2RG5

Note The listed DDR5-6400 DIMMs are supported with 4th Gen and 5th Gen AMD EPYC CPUs on Cisco UCS X215c M8 Compute Node and Cisco UCS C245 M8 and C225 M8 Rack servers.

- Added support for the following DDR5 Dual Inline Memory Modules (DIMMs), rated for a memory transfer speed of 6400 MT/s on Cisco UCS X210c M7 Compute Node and Cisco UCS C240 M7 and C220 M7 Rack servers:
  - UCS-MRX16G1RE5
  - UCS-MRX32G1RE5
  - UCS-MR128G2RG5

Note The listed DDR5-6400 DIMMs are supported with 5th Gen Intel® Xeon® Scalable Processors on Cisco UCS X210c M7 Compute Node and Cisco UCS C240 M7 and C220 M7 Rack servers.

New hardware in Cisco UCS B-Series M5 6.0(1.260031) Server Firmware Release — None

New hardware in Cisco UCS X-Series M8, M7 6.0(2.260143) and C-Series M8 6.0(2.260143) Server Firmware Release

- Support for UCSX-GPU-L40S Graphics Processing Unit (GPU) on Cisco UCS X210c M7 server when used with the X580p PCIe node.
- Support for NVIDIA RTX Pro 4500 GPU 160W 32GB Gen5 FHFL 1-slot (UCSX-GPU-RTXP4500) with Cisco UCS C245 M8 and C240 M8 servers.
- Support for NVIDIA RTX Pro 6000D GPU 600W, 84GB, 2-slot FHFL PCIe GPU (UCSC-GPU-RTX6000D) with Cisco UCS C240 M8 servers.
- Support for NVIDIA RTX Pro 4500 GPU (UCSX-GPU-RTXP4500) on Cisco UCS X580p PCIe node with Cisco UCS X210c M7, Cisco UCS X215c M8, and X210c M8 servers.
- Support for 15.3 TB Micron 7500 drive on Cisco UCS X410c M8 servers.

New hardware in Cisco UCS X-Series M8, M7 6.0(2.260069) and C-Series M8 6.0(2.260069) Server Firmware Release

- Support for NVIDIA OEM BlueField-3 B3220 DPU 2x200G QSFP112, Crypto Disabled (UCSC-P-N3220) on Cisco UCS C245 M8 and C240 M8 and C240 M7 servers.
- Support for NVIDIA BlueField-3 B3220L SuperNIC 2x200G QSFP112, PCIe Gen5.0 x16, Crypto Disabled (UCSC-P-N3220L) on Cisco UCS C225 M8, C245 M8, C220 M8, C240 M8 and C240 M7 servers.
- Support for NVIDIA Crypto B3220 Data Processing Unit (DPU) (UCSC-P-NC3220) on Cisco UCS C245 and C240 M8 servers.
- Support for 30 TB E3.S TLC Micron 9550 drive on Cisco UCS C240, C220, X215c, and X210c M8 servers.
- Support for E3.S FIPS (Kioxia CM-7) drives on Cisco UCS C240, C220, X215c, and X210c M8 servers.

New hardware in Cisco UCS B-Series M5 6.0(1.260012) Server Firmware Release — None

New hardware in Cisco UCS X-Series M8, M7 Server Firmware Release, 6.0(2.260040)

- **X-Series M8 6.0(2.260040) Server Firmware**

  Cisco UCS X410c M8 Compute Node

  A Cisco UCS X410c M8 compute node is a second-generation, four-socket compute node that is purpose-built for the Cisco UCS X-Series Modular System.

  The 7-rack-unit (7-RU) Cisco UCS X9508 server chassis supports up to four Cisco UCS X410c M8 compute nodes. This configuration provides the flexibility to adapt to diverse workloads.

  The Cisco UCS X410c M8 compute node provides these main features:

  - **CPU**: Four Intel Xeon 6 processors with up to 86 cores per processor.
  - **Memory**: Up to 16 TB of main memory using 64 256-GB DDR5-6400 DIMMs.
  - **Storage**: The node supports these storage configurations:
    - Up to nine hot-pluggable EDSFF E3.S NVMe drives with a passthrough front mezzanine controller.
    - Up to six hot-pluggable 2.5-inch Solid-State Drives (SSDs) or Non-Volatile Memory Express (NVMe) drives with enterprise-class RAID options.
    - Up to two M.2 SATA or NVMe drives for boot and local storage.
  - **mLOM virtual interface cards (VICs)**: The node supports these modular LAN on motherboard (mLOM) options:
    - Cisco UCS VIC 15420: Enables up to 50 Gbps (2 x 25 Gbps) of unified fabric connectivity to each intelligent fabric module (IFM).
    - Cisco UCS VIC 15230: Enables up to 100 Gbps of unified fabric connectivity to each IFM.
  - **Optional mezzanine card**: The optional 5th-Gen Cisco UCS VIC 15422 occupies the mezzanine slot. A bridge card extends the network connections to provide a total bandwidth of 200 Gbps per server.
  - **Security**: Support for an optional Trusted Platform Module (TPM), a secure boot FPGA, and ACT2 anti-counterfeit provisions.

  For more information, see Cisco UCS X410c M8 Compute Node Data Sheet and Cisco UCS X410c M8 Compute Node Spec Sheet.

- **X-Series M7 6.0(2.260040) Server Firmware**

Support for Cisco UCS X580p PCIe Node with Cisco UCS X210c M7 servers

Added support for Cisco UCS X580p PCIe Node with Cisco UCS X210c M7 servers. The UCSX-GPU-H200-NVL and UCSX-GPU-RTXP6000 GPUs are supported on the Cisco UCS X210c M7 server when used with the X580p PCIe node.

Note

- The UCSX-GPU-L40S GPU is currently not supported on the Cisco UCS X210c M7 server when used with the X580p PCIe node.
- Support for the Cisco UCS X210c M7 server with the X580p PCIe node is available only when using 5th Generation Intel Xeon Scalable processors (Emerald Rapids).

New hardware in Cisco UCS XE-Series M8 Server Firmware Release, 6.0(1.260001) — None

New hardware in Cisco UCS C-Series M8 6.0(1.250194) Server Firmware Release — None

New hardware in Cisco UCS X-Series M8 6.0(1.252114), M7, M6 6.0(1.250179), B-Series M6, M5 6.0(1.250169), and C-Series M8, M7, M6 6.0(1.250192) Server Firmware Release — None

New hardware in Cisco UCS XE-Series M8 Server Firmware Release, 6.0(1.251030)

Cisco UCS XE130c M8 Compute Node

Cisco Unified Edge brings together computing, storage, routing, switching, and security into a single configurable solution to help IT organizations simplify the deployment, operations, and lifecycle management of edge infrastructure at global scale.

Cisco Unified Edge is a modular edge platform, with a 3RU, short-depth, multi-mountable chassis with features to operate in extended temperature range (5°C to 45°C), maintain a quiet acoustic profile (40s dBA at 25°C and 20% PWM), and offer protection against high particulate environments, allowing deployments in a wide range of physical spaces.

The Cisco UCS XE130c M8 is a family of 1RU, half-width compute nodes; up to five Cisco UCS XE130c M8 compute nodes can be housed inside a Cisco UCS XE9305 chassis. It delivers enterprise class performance, versatility and density but in a compact edge-optimized form factor.

Key Features and Benefits

- **Form factor and chassis:**
  - 1RU-high and half-width compute node
  - The Cisco UCS XE130c M8 compute node mounts in a Cisco UCS XE9305 chassis
- **CPU:** One Intel® Xeon® 6 System on a Chip (SoC) with Performance-cores (P-cores) Processor, with 12, 20, or 32 physical cores.
- **Memory:**
  - 8 total DDR5 DIMM Slots, at up to 6400 MT/s RDIMMs
  - Up to 768GB of main memory with eight 96 GB DDR5-6400 DIMMs
- **GPU:** One dedicated PCIe Gen5 GPU slot for a half-height, half-length GPU.
- **Networking:**
  - Two integrated 25 Gbps host ports connecting via chassis mid-plane to the embedded switches on both Cisco UCS XE chassis management controllers.
  - Two integrated 1/10 Gbps RJ45 host ports.
- **Storage:**

  There are two types of flash storage options simultaneously available in the Cisco UCS XE130c M8 compute node:
  - Internal M.2 SSDs: Up to two M.2 SSDs protected by hardware RAID 1
  - Front-Facing E3.S NVMe Drives
- **PCIe adapter:** One PCIe Gen5 slot for a half-height, half-length PCIe adapter requires IO-optimized configuration, which includes three front-panel hot-swappable E3.S NVMe drives, each supporting up to15 TB.
- **Front panel interfaces:**
  - One KVM connector
  - One USB-C console port for UART connection to the IMC
- **Power subsystem:** Power is supplied from the Cisco UCS XE9305 chassis power supplies. The Cisco UCS XE130c M8 Compute Node consumes a maximum of 425W.
- **Fans:** Integrated in the Cisco UCS XE9305 chassis.
- **Integrated management processor:**
  - The built-in Cisco Integrated Management Controller enables monitoring of Cisco UCS XE130c M8 Compute Node inventory, health, and system event logs.

    - ASPEED AST2600

- **Firmware standards:**
    - UEFI Spec 2.9
    - ACPI 6.5
    - SMBIOS Ver 3.7
- **Front indicators:**
    - Power button and indicator
    - System activity indicator
    - Location button and indicator
- **Security:** The server has an onboard Trusted Platform Module (TPM) connected to the server's Baseboard Management Controller (BMC), which acts as secure key storage and also assists in anti-counterfeit protection. Additionally, the server supports an optional TPM for the host system.

For more information, see Cisco UCS XE130c M8 Compute Node Data Sheet and Release Notes for Cisco Intersight Unified Edge eCMC Infrastructure Firmware Release, 6.0.

Debug Capability Test for Cisco UCS XE-Series M8 Server

Please choose the method that corresponds to your connection setup.

Method 1: Using a Direct USB-C Connection

You can plug a USB-C cable directly into the console port on the front of the server. The detailed steps provided under **Method 2** are specific to the debug breakout cable and do not apply to this direct connection method.

Method 2: Using the Debug Breakout Cable (UCSX-C-DEBUGCBL)

Follow these steps to use the serial port for Server Debug Capability testing when using the debug breakout cable UCSX-C-DEBUGCBL:

1. **Connect the Serial Cable:**
    a. Use a DB9 serial cable or a USB-to-Serial adapter as needed.
    b. Connect the cable from the server's serial port to your debug console or host syste.
2. **Configure BIOS/UEFI Settings:**
    a. Access the server BIOS/UEFI during boot.
    b. Enable the **Serial Console Redirection** option.
    c. Set the baud rate (typically 115200), data bits (8), parity (None), and stop bits (1).
3. **Launch Serial Terminal:**
    a. Use terminal emulation tools such as PuTTY, Tera Term, or minicom.
    b. Select the correct COM port corresponding to your serial connection.

c. Match the baud rate and other serial settings configured in BIOS.

4. **Verify Output:**
   a. Reboot the server and observe the serial console for POST messages and system logs.
   b. Confirm you can interact with the system if needed (e.g., login prompt or shell access).
5. **Log and Capture:**
   a. Enable logging in your terminal tool to capture debug output for later analysis.
   b. Save logs with timestamps for traceability.
6. **Troubleshooting:**
   a. If no output appears, verify cable connections, BIOS settings, and COM port configuration.
   b. Ensure no other service or application is occupying the serial port.

New hardware in Cisco UCS X-Series M8 Server Firmware Release, 6.0(1.252039)

This section provides a brief description of the new hardware features.

Cisco UCS X580p PCIe Node

The Cisco UCS X580p PCIe Node is the latest PCIe resource node for the UCS X-Series Modular System. It delivers high-performance GPU support for workloads such as generative and agentic AI fine-tuning, inference, and other applications that require GPU acceleration.

The Cisco UCS X580p PCIe Node supports up to four PCIe GPUs. It can be paired with the Cisco UCS X210c M8 server (with Intel® Xeon® processors) or the UCS X215c M8 server (with EPYC processors). The X580p uses Cisco UCS X-Fabric technology for GPU connectivity.

The X580p occupies two node slots in the X-Series chassis and allows assignment of up to four GPUs per node. Each 7RU Cisco UCS X9508 chassis supports up to two PCIe Nodes, with each node pairing with one or two servers.

For more information, see Cisco UCS X580p PCIe Node Installation and Service Guide and Cisco UCS X580p PCIe Node Spec Sheet.

Cisco UCS X9516 X-Fabric

The Cisco UCS X9516 X-Fabric is the second-generation X-Fabric module for the UCS X9508 chassis. It provides ultra-low-latency PCIe Gen5 switching and SmartNIC support, enabling flexible and composable IT resources. Managed via Cisco Intersight®, the UCS X9516 X-Fabric allows GPUs and NICs to be dynamically provisioned across servers using policy-based management.

Paired with the UCS X580p PCIe Node, the X9516 X-Fabric supports up to four dual-slot GPUs per node with NVLink Bridge support, serving as the control point for modular GPU composability in AI-driven environments.

For more information, see Cisco UCS X9516 X-Fabric Data Sheet.

Minimum Firmware Requirements to Support Cisco UCS X580p PCIe Node and Cisco UCS X9516 X-Fabric

- X580p PCIe Node Firmware: 6.0(1.252044)
- X9508 Chassis Firmware: 6.0(1.252044)
- Cisco UCS X-Series M8 Server Firmware: 6.0(1.252039)
- Fabric Interconnect Infrastructure Firmware: 6.0(1.250229)

Note The X580p PCIe Node firmware 6.0(1.252044) and X9508 Chassis firmware 6.0(1.252044) are available as separate bundles.

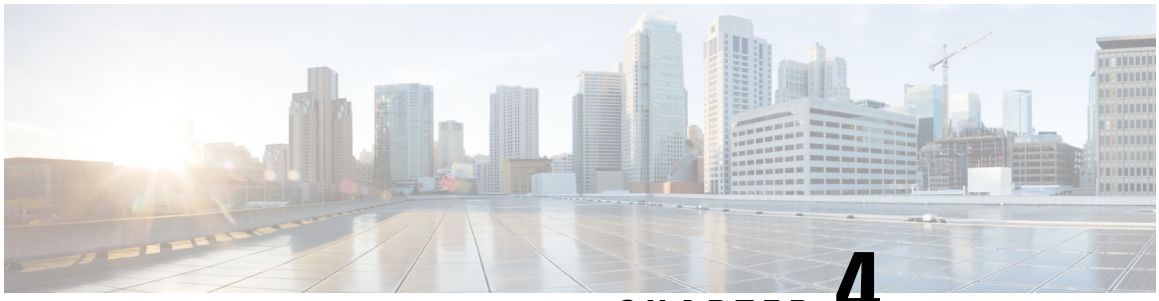
New hardware in Cisco UCS X-Series M8, M7, M6 6.0(1.250162), B-Series M6, M5 6.0(1.250157), and C-Series M8, M7, M6 6.0(1.250174) Server Firmware Release — None

New hardware in Cisco UCS X-Series M8, M7, M6 6.0(1.250122), B-Series M6, M5 6.0(1.250127), and C-Series M8, M7, M6 6.0(1.250131) Server Firmware Release — None

New hardware in Cisco UCS X-Series M8, M7, M6 6.0(1.250120) and C-Series M8, M7, M6 6.0(1.250127) Server Firmware Release

- Support for 30TB 2.5 inch QLC drive on Cisco UCS C225 M8 servers.
- Support for next generation large form factor (3.5-inch) hard disk drives on Cisco UCS C-Series M8 and C240L M6 servers.
- Dual support for the Cisco Tri-Mode M1 24G RAID (UCSC-RAID-M1L16) controllers on Cisco UCS C240 M8 Servers, enabling independent configuration and management of two controllers within the same server environment.
- Starting with the Infra Firmware release 6.0(1), Cisco UCS X-Series and C-Series servers support Cisco UCS 6664 Fabric Interconnects.

  For more information, see Release Notes for Cisco Intersight Managed Mode Infrastructure Firmware, Release 6.0.



CHAPTER 4

Security fixes

You can view the open issues, resolved issues, and security fixes using the Cisco Bug Search Tool.

- Security fixes in Cisco UCS C-Series C220 M8 and C240 M8 6.0(2.260236) Server Firmware Release — None, on page 24
- Security fixes in Cisco UCS C-Series M8, M7, M6 6.0(2.260205) and B-Series M6 6.0(2.260205) Server Firmware Release — None, on page 24
- Security fixes in Cisco UCS X-Series M8, M7 6.0(2.260180) and C-Series M8, M7 6.0(2.260180) Server Firmware Release — None, on page 24
- Security fixes in Cisco UCS B-Series M5 6.0(1.260031) Server Firmware Release, on page 24
- Security fixes in Cisco UCS C-Series M8, M7, M6 6.0(2.260143) and B-Series M6 6.0(2.260143) Server Firmware Release, on page 24
- Security fixes in Cisco UCS X-Series M8, M7, M6 6.0(2.260069), C-Series M8, M7, M6 6.0(2.260069), and B-Series M6 6.0(2.260069) Server Firmware Release, on page 25
- Security fixes in Cisco UCS B-Series M5 6.0(1.260012) Server Firmware Release, on page 25
- Security fixes in Cisco UCS X-Series M8, M7, M6 6.0(2.260040), XE-Series M8 6.0(2.260042), C-Series M8, M7, M6 6.0(2.260044), and B-Series M6 6.0(2.260040) Server Firmware Release, on page 26
- Security fixes in Cisco UCS XE-Series M8 Server Firmware Release, 6.0(1.260001) — None, on page 42
- Security fixes in Cisco UCS C-Series M8 6.0(1.250194) Server Firmware Release — None, on page 42
- Security fixes in Cisco UCS X-Series M8 6.0(1.252114), M7, M6 6.0(1.250179), B-Series M6, M5 6.0(1.250169), and C-Series M8, M7, M6 6.0(1.250192) Server Firmware Release — None, on page 42
- Security fixes in Cisco UCS XE-Series M8 6.0(1.251030) Server Firmware Release — None, on page 42
- Security fixes in Cisco UCS X-Series M8 6.0(1.252039) Server Firmware Release — None, on page 42
- Security fixes in Cisco UCS C-Series M8, M7, M6 6.0(1.250174) Server Firmware Release, on page 42
- Security fixes in Cisco UCS X-Series M8, M7, M6 6.0(1.250122), B-Series M6, M5 6.0(1.250127), and C-Series M8, M7, M6 6.0(1.250131) Server Firmware Release — None, on page 43
- Security fixes in Cisco UCS X-Series M8, M7, M6 6.0(1.250120), B-Series M6, M5 6.0(1.250126), and C-Series M8, M7, M6 6.0(1.250127) Server Firmware Release, on page 43

Security fixes in Cisco UCS C-Series C220 M8 and C240 M8 6.0(2.260236) Server Firmware Release — None

Security fixes in Cisco UCS C-Series M8, M7, M6 6.0(2.260205) and B-Series M6 6.0(2.260205) Server Firmware Release — None

Security fixes in Cisco UCS X-Series M8, M7 6.0(2.260180) and C-Series M8, M7 6.0(2.260180) Server Firmware Release — None

Security fixes in Cisco UCS B-Series M5 6.0(1.260031) Server Firmware Release

Defect ID - CSCwt77804

A vulnerability in the Unified Extensible Firmware Interface (UEFI) Shell implementation of all Cisco UCS B-series M5 servers could allow an authenticated attacker with valid credentials for a user account with the role of *user* or *admin* or an unauthenticated attacker with physical access to an affected device to bypass UEFI Secure Boot validation checks and execute unauthorized software.

This vulnerability is due to the availability of memory write commands in the UEFI Shell while UEFI Secure Boot is enabled on a device. An attacker could exploit this vulnerability by selecting the UEFI Shell boot option at boot time and using available shell commands to modify UEFI memory variables. A successful exploit could allow the attacker to manipulate the preboot environment, overwrite UEFI Secure Boot-related memory values, and execute unauthorized software on the affected device.

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

This advisory is available at the following link:

Cisco UCS and UCS-Based Appliances UEFI Shell Secure Boot Bypass Vulnerability

Security fixes in Cisco UCS C-Series M8, M7, M6 6.0(2.260143) and B-Series M6 6.0(2.260143) Server Firmware Release

Defect ID - CSCwt77804

A vulnerability in the Unified Extensible Firmware Interface (UEFI) Shell implementation of all Cisco UCS B-series and C-series M6, M7, and M8 servers could allow an authenticated attacker with valid credentials

for a user account with the role of *user* or *admin* or an unauthenticated attacker with physical access to an affected device to bypass UEFI Secure Boot validation checks and execute unauthorized software.

This vulnerability is due to the availability of memory write commands in the UEFI Shell while UEFI Secure Boot is enabled on a device. An attacker could exploit this vulnerability by selecting the UEFI Shell boot option at boot time and using available shell commands to modify UEFI memory variables. A successful exploit could allow the attacker to manipulate the preboot environment, overwrite UEFI Secure Boot-related memory values, and execute unauthorized software on the affected device.

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

This advisory is available at the following link:

Cisco UCS and UCS-Based Appliances UEFI Shell Secure Boot Bypass Vulnerability

Security fixes in Cisco UCS X-Series M8, M7, M6 6.0(2.260069), C-Series M8, M7, M6 6.0(2.260069), and B-Series M6 6.0(2.260069) Server Firmware Release

Defect ID - CSCwr69876

This product includes third-party software that is affected by the vulnerabilities identified by the following Common Vulnerabilities and Exposures (CVE) IDs:

CVE ID	Description
CVE-2025-0033	Improper access control within AMD SEV-SNP could allow an admin privileged attacker to write to the RMP during SNP initialization, potentially resulting in a loss of SEV-SNP guest memory integrity.
CVE-2025-29943	Improper write condition handling within AMD CPUs could allow an admin-privileged attacker to modify the configuration of the CPU pipeline, potentially resulting in the corruption of the stack pointer inside an SEV-SNP guest.
CVE-2025-48514	Insufficient Granularity of Access Control in SEV firmware can allow a privileged attacker to create a SEV-ES Guest to attack SNP guest, potentially resulting in a loss of confidentiality.

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 Cisco UCS B-Series M5 6.0(1.260012) Server Firmware Release

Defect ID - CSCwq34278

This product includes third-party software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

CVE ID	Description
CVE-2025-20064	Improper input validation in the UEFI FlashUcAcmSmm module on certain Intel reference platforms may allow a privileged local attacker to execute arbitrary code and escalate privileges, severely impacting system confidentiality, integrity, and availability.
CVE-2025-20027	Improper input validation in the UEFI WheaERST module on certain Intel reference platforms may allow a privileged local attacker to escalate privileges, potentially impacting system confidentiality, integrity, and availability.
CVE-2025-20028	A time-of-check time-of-use (TOCTOU) race condition in the UEFI WheaERST SMM module on certain Intel reference platforms may allow a privileged local attacker to escalate privileges, impacting system confidentiality, integrity, and availability.
CVE-2025-20105	Improper input validation in certain UEFI firmware SMM modules on Intel reference platforms may allow a privileged local attacker to execute arbitrary code with low complexity, resulting in a high impact on system confidentiality, integrity, and availability.

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 Cisco UCS X-Series M8, M7, M6 6.0(2.260040), XE-Series M8 6.0(2.260042), C-Series M8, M7, M6 6.0(2.260044), and B-Series M6 6.0(2.260040) Server Firmware Release

Defect ID - CSCwr50426

This product includes third-party software that is affected by the vulnerabilities identified by the following Common Vulnerabilities and Exposures (CVE) IDs:

CVE ID	Description
CVE-2024-13176	A timing side-channel vulnerability in OpenSSL's ECDSA signature computation may allow an attacker with local access or a low-latency network connection to potentially recover a private key, particularly when using the NIST P-521 curve.
CVE-2024-5535	A buffer overread flaw in OpenSSL's SSL_select_next_proto API function, triggered when called with an empty client protocols buffer, may cause an application crash or allow up to 255 bytes of private memory to be sent to a peer.

CVE ID	Description
CVE-2024-9143	Use of low-level GF(2^m) elliptic curve APIs in OpenSSL with untrusted explicit values for the field polynomial can lead to out-of-bounds memory reads or writes, potentially resulting in an application crash or remote code execution.

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.

Defect ID - CSCwr81218

This product includes third-party software that is affected by the vulnerabilities identified by the following Common Vulnerabilities and Exposures (CVE) IDs:

CVE ID	Description
CVE-2025-48384	A link following vulnerability in Git stems from inconsistent handling of carriage return characters in configuration files; when initializing a submodule with a trailing carriage return in its path, the altered path may lead to an incorrect checkout location, potentially allowing arbitrary code execution if a symlink points to a malicious hook script.

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.

Defect ID - CSCwr83710

This product includes third-party software that is affected by the vulnerabilities identified by the following Common Vulnerabilities and Exposures (CVE) IDs:

CVE ID	Description
CVE-2021-0920	A race condition in the Unix domain socket implementation (unix_scm_to_skb inaf_unix.c) of the Linux kernel may lead to a use-after-free vulnerability, allowing a local attacker to potentially escalate privileges or cause a system crash.
CVE-2024-53150	An out-of-bounds read vulnerability in the Linux kernel's ALSA USB-audio driver, caused by insufficient validation of descriptor lengths (bLength), may allow an attacker with physical access to use a malicious USB device to disclose sensitive kernel memory or cause a denial of service.
CVE-2025-38352	A race condition in the Linux kernel's POSIX CPU timer handling between the handle_posix_cpu_timers() and posix_cpu_timer_del() functions may result in a use-after-free scenario, potentially allowing a local user to escalate privileges or crash the system.

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.

Defect ID - CSCws61975

This product includes third-party software that is affected by the vulnerabilities identified by the following Common Vulnerabilities and Exposures (CVE) IDs:

CVE ID	Description
CVE-2015-5477	An error in the handling of TKEY queries in ISC BIND 9 can be exploited by a remote attacker to trigger a REQUIRE assertion failure, causing the named daemon to exit and resulting in a denial of service.
CVE-2016-2776	A flaw in the way ISC BIND 9 constructs responses to specific queries can lead to an assertion failure in buffer.c, allowing a remote attacker to cause the named process to crash and exit unexpectedly.
CVE-2023-50387	Known as **KeyTrap**, this vulnerability in DNSSEC-validating resolvers (such as BIND and Unbound) allows a remote attacker to cause extreme CPU exhaustion and a denial of service by providing a specially crafted DNSSEC-signed zone with complex resource record combinations.

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.

Defect ID - CSCws65661

This product includes third-party software that is affected by the vulnerabilities identified by the following Common Vulnerabilities and Exposures (CVE) IDs:

CVE ID	Description
CVE-2010-2252	Wget 1.12 and earlier allows remote attackers to write to arbitrary files via a 302 redirect to a URL with a different filename when the -O (output document) option is used, as Wget uses the filename from the redirected URL rather than the original.
CVE-2014-4877	Wget before 1.16 allows remote FTP servers to write to arbitrary files, and potentially execute code, via a symlink attack in a directory listing during a recursive retrieval.
CVE-2016-4971	Wget before 1.18 allows remote servers to write to arbitrary files by redirecting an HTTP request to an FTP URL, which causes Wget to save the file with a name provided by the FTP server rather than the original HTTP filename.
CVE-2017-6508	Wget before 1.19.1 allows remote attackers to inject arbitrary HTTP headers (CRLFinjection) via a crafted URL, which could lead to session hijacking or other header-based attacks.
CVE-2018-0494	Wget before 1.19.5 allows remote attackers to bypass intended cookie access restrictions via a malformed Set-Cookie header, potentially leading to cookie injection or overwriting.
CVE-2021-31879	Wget before 1.21.1 does not properly handle certain HTTP response headers, such as Content-Length, which may allow a remote attacker to bypass security controls or cause unexpected behavior.
CVE-2024-10524	A path traversal vulnerability exists in certain versions of WPS Office for Windows that allows an attacker to achieve arbitrary code execution via a specially crafted file.

CVE ID	Description
CVE-2024-38428	Wget before 1.24.5 is vulnerable to a flaw where it fails to properly parse user info in a URI, which could be exploited to bypass security filters or lead to credential disclosure in certain configurations.

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.

Defect ID - CSCws68419

This product includes third-party software that is affected by the vulnerabilities identified by the following Common Vulnerabilities and Exposures (CVE) IDs:

CVE ID	Description
CVE-2009-5155	An off-by-one error in the strfmon_l function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a large precision value.
CVE-2010-0015	The NIS+ implementation in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted NIS+ directory name that triggers a buffer overflow.
CVE-2011-5320	The tar implementation in BusyBox before 1.20.0 allows remote attackers to create or overwrite arbitrary files via a directory traversal attack in a tar header.
CVE-2012-4412	An integer overflow in the strcoll function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long string.
CVE-2012-4424	A stack-based buffer overflow in the strcoll function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long string.
CVE-2013-4237	The read dir_r function in the GNU C Library (glibc) does not properly handle certain directory entries, which allows context-dependent attackers to cause a denial of service (out-of-bounds read and crash).
CVE-2013-4458	A stack-based buffer overflow in the getaddrinfo function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) via a large number of AF_INET6 addresses.
CVE-2013-4788	The PTR_MANGLE implementation in the GNU C Library (glibc) does not properly initialize the guard value, which allows local attackers to bypass the pointer-guarding protection mechanism.
CVE-2014-4043	The posix_spawn_file_actions_addopen function in the GNU C Library (glibc) before 2.20 does not copy its path argument, which allows context-dependent attackers to trigger a use-after-free vulnerability.
CVE-2014-6040	An out-of-bounds read in the iconv function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) via a crafted multibyte sequence.

CVE ID	Description
CVE-2014-7817	The wordexp function in the GNU C Library (glibc) allows context-dependent attackers to execute arbitrary commands via a crafted string that triggers command substitution even when WRDE_NOCMD is specified.
CVE-2014-8121	The nss_files implementation in the GNU C Library (glibc) does not properly handle certain database files, which allows local attackers to cause a denial of service (infinite loop) or corrupt the database.
CVE-2014-9402	The getnetbyname function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (infinite loop) via a crafted DNS response.
CVE-2014-9761	A stack-based buffer overflow in the nan function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) via a long string.
CVE-2015-1781	A buffer overflow in the gethostbyname_r function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long host name.
CVE-2015-5180	A NULL pointer dereference in the res_query function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) via a crafted DNS response.
CVE-2015-8776	An out-of-bounds access in the strftime function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) via a crafted format string.
CVE-2015-8777	The LD_POINTER_GUARD environment variable in the GNU C Library (glibc) allows local attackers to bypass the pointer-guarding protection mechanism by disabling it.
CVE-2015-8778	An integer overflow in the hcreate function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a large number of elements.
CVE-2015-8779	A stack-based buffer overflow in the catopen function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long catalog name.
CVE-2015-8982	A buffer overflow in the strftime function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) via a crafted format string.
CVE-2015-8983	An integer overflow in the _IO_wstr_overflow function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a large string.
CVE-2015-8984	An out-of-bounds read in the fnmatch function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) via a crafted pattern.

CVE ID	Description
CVE-2015-8985	The pop_fail_stack function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (assertion failure and crash) via vectors related to extended regular expression processing.
CVE-2016-10228	An out-of-bounds write in the iconv function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted multibyte sequence.
CVE-2016-10739	A buffer overflow in the getaddrinfo function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) via a large number of AF_INET6 addresses.
CVE-2016-1234	A stack-based buffer overflow in the glob function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long path.
CVE-2016-3075	A stack-based buffer overflow in the getnetbyname function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) via a crafted DNS response.
CVE-2016-3706	A stack-based buffer overflow in the getaddrinfo function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) via vectors involving hostent conversion, due to an incomplete fix for CVE-2013-4458.
CVE-2016-4429	A stack-based buffer overflow in the clntudp_call function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) via a crafted RPC response.
CVE-2017-12132	The DNS stub resolver in the GNU C Library (glibc) before 2.26 will solicit largeUDP responses when EDNS support is enabled, potentially simplifying off-path DNS spoofing attacks due to IP fragmentation.
CVE-2017-15670	An off-by-one error in the glob function in the GNU C Library (glibc) before 2.27leads to a heap-based buffer overflow when processing home directories using the ~ operator followed by a long string.
CVE-2017-15671	The glob function in the GNU C Library (glibc) before 2.27 could skip freeing allocated memory when processing the ~ operator with a long username, potentially leading to a denial of service (memory leak).
CVE-2017-16997	The elf/dl-load.c implementation in the GNU C Library (glibc) does not properly handle certain checks, which allows local attackers to bypass security restrictions via a crafted shared object.
CVE-2017-8804	The memmove and memcpy implementations in the GNU C Library (glibc) for x86_64 do not properly handle overlapping memory regions in certain cases, which allows context-dependent attackers to cause a denial of service (crash) or possibly have other unspecified impact.
CVE-2018-1000001	A buffer underflow in the realpath function in the GNU C Library (glibc) allows local attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted path.

CVE ID	Description
CVE-2018-11236	An integer overflow in the __vfprintf_internal function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a large precision value.
CVE-2018-6485	An integer overflow in the implementation of the posix_memalign in memalign functions in the GNU C Library (glibc) 2.26 and earlier could cause these functions to return a pointer to a heap area that is too small, potentially leading to heap corruption.
CVE-2019-1010023	A buffer overflow in the ld.so dynamic loader in the GNU C Library (glibc) allows local attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted environment variable.
CVE-2019-19126	The GNU C Library (glibc) before 2.31 does not properly handle the LD_PRELOAD environment variable for SUID binaries, which allows local attackers to bypass security restrictions.
CVE-2019-25013	A buffer overflow in the iconv function in the GNU C Library (glibc) when converting to the EUC-KR character set allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code.
CVE-2019-9169	A heap-based buffer overflow in the regexec function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted regular expression.
CVE-2020-10029	A stack-based buffer overflow in the cosl function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a large input value.
CVE-2020-1751	A stack-based buffer overflow in the _dl_open function in the GNU C Library (glibc) allows local attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted shared object path.
CVE-2020-1752	A use-after-free vulnerability in the glob function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted path.
CVE-2020-27618	A buffer overflow in the iconv function in the GNU C Library (glibc) when converting to the IBM1364 character set allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code.
CVE-2020-29573	A buffer overflow in the printf function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) via a large precision value.
CVE-2021-27645	A double-free vulnerability in the nscd (name service cache daemon) in the GNU C Library (glibc) allows local attackers to cause a denial of service (crash) or possibly execute arbitrary code.
CVE-2021-3326	A buffer overflow in the iconv function in the GNU C Library (glibc) when converting to the ISO-2022-JP-3 character set allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code.

CVE ID	Description
CVE-2021-33574	A use-after-free vulnerability in the mq_notify function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code.
CVE-2021-35942	A buffer overflow in the wordexp function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) via a long string.
CVE-2021-3999	A buffer overflow in the getcwd function in the GNU C Library (glibc) allows local attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long path.
CVE-2022-23218	A stack-based buffer overflow in the svcunix_create function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) via a crafted RPC request.
CVE-2022-23219	A stack-based buffer overflow in the clnt_create function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) via a crafted RPC request.
CVE-2023-4527	A stack-based buffer overflow in the getaddrinfo function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) via a large DNS response received over TCP.
CVE-2023-4806	A use-after-free vulnerability in the getaddrinfo function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) via a crafted DNS response.
CVE-2023-4813	A use-after-free vulnerability in the getaddrinfo function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) via a crafted DNS response.
CVE-2023-4911	A buffer overflow in the GNU C Library's dynamic loader ld.so while processing the GLIBC_TUNABLES environment variable allows a local attacker to execute arbitrary code with elevated privileges.
CVE-2023-5156	A memory leak in the getaddrinfo function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (memory exhaustion) via a crafted DNS response.
CVE-2024-2961	A buffer overflow in the iconv function in the GNU C Library (glibc) when converting to the ISO-2022-CN-EXT character set allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code.
CVE-2024-33599	A buffer overflow in the nscd (name service cache daemon) in the GNU C Library (glibc) allows local attackers to cause a denial of service (crash) or possibly execute arbitrary code.
CVE-2024-33600	A NULL pointer dereference in the nscd (name service cache daemon) in the GNU C Library (glibc) allows local attackers to cause a denial of service (crash) via a crafted request.

CVE ID	Description
CVE-2024-33601	A buffer overflow in the nscd (name service cache daemon) in the GNU C Library (glibc) allows local attackers to cause a denial of service (crash) or possibly execute arbitrary code.
CVE-2024-33602	CVE-2024-33602A buffer overflow in the nscd (name service cache daemon) in the GNU C Library (glibc) allows local attackers to cause a denial of service (crash) or possibly execute arbitrary code.
CVE-2025-0395	A buffer overflow in the assert() function in the GNU C Library (glibc) versions 2.13 to 2.40 occurs because insufficient space is allocated for the failure message, potentially leading to a denial of service.
CVE-2025-4802	A vulnerability in the GNU C Library (glibc) versions 2.27 to 2.38 allows a local attacker to load malicious shared libraries and escalate privileges via an untrusted LD_LIBRARY_PATH in statically compiled setuid binaries that call dlopen.
CVE-2025-5702	A vulnerability in the optimized strcmp implementation for Power10 processors in the GNU C Library (glibc) version 2.39 and later improperly initializes vector registers, potentially leading to data corruption or altered control flow.
CVE-2025-8058	A double-free vulnerability in the regcomp function in the GNU C Library (glibc) versions 2.4 to 2.41 occurs during bracket expression parsing when a memory allocation failure takes place, potentially allowing arbitrary code execution.

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.

Defect ID - CSCws68836

This product includes third-party software that is affected by the vulnerabilities identified by the following Common Vulnerabilities and Exposures (CVE) IDs:

CVE ID	Description
CVE-2007-5116	A buffer overflow in the polymorphic opcode support in the Regular Expression Engine (regcomp.c) in Perl 5.8 allows context-dependent attackers to execute arbitrary code by switching from byte to Unicode (UTF) characters in a regular expression.
CVE-2008-1927	A double free vulnerability in Perl 5.8.8 allows context-dependent attackers to cause a denial of service (memory corruption and crash) via a crafted regular expression containing UTF-8characters.
CVE-2008-5302	A race condition in the rmtree function in File::Path in Perl 5.8.8 and 5.10.0 allows local users to create arbitrary setuid binaries via a symlink attack.
CVE-2008-5303	A race condition in the rmtree function in File::Path in Perl 5.8.8 allows local users to delete arbitrary files via a symlink attack, representing a regression of a previous security fix.

CVE ID	Description
CVE-2010-1168	The Safe (aka Safe.pm) module before 2.25 for Perl allows context-dependent attackers to bypass intended access restrictions and execute arbitrary code via vectors involving implicitly called methods such as DESTROY and AUTOLOAD.
CVE-2010-1447	The Safe (aka Safe.pm) module 2.26 and earlier for Perl allows context-dependent attackers to bypass access restrictions and execute arbitrary code via vectors involving subroutine references and delayed execution.
CVE-2010-2761	The multipart_init function in CGI.pm before 3.50 uses a hardcoded MIME boundary string, which allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks.
CVE-2010-4410	A CRLF injection vulnerability in the header function in CGI.pm before 3.50 allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via newline characters.
CVE-2011-0761	Perl 5.10.x allows context-dependent attackers to cause a denial of service (NULL pointer dereference and crash) by injecting arguments into functions such as getpeername, readdir, and closedir.
CVE-2011-1487	The lc, lcfirst, uc, and ucfirst functions in Perl 5.10.x through 5.13.x do not apply the taint attribute to return values, allowing attackers to bypass taint protection mechanisms via crafted strings.
CVE-2011-2939	An off-by-one error in the decode_xs function in the Encode module for Perl allows context-dependent attackers to cause a denial of service (memory corruption) or execute arbitrary code via a crafted Unicode string.
CVE-2011-3597	An eval injection vulnerability in the Digest module before 1.17 for Perl allows context-dependent attackers to execute arbitrary commands via the new constructor.
CVE-2011-4116	The _is_safe function in the File::Temp module for Perl does not properly handle symlinks, which could allow a local attacker to bypass security checks.
CVE-2012-5195	A heap-based buffer overflow in the Perl_repeatcpy function in Perl allows context-dependent attackers to cause a denial of service or execute arbitrary code via the 'x' string repeat operator.
CVE-2012-5526	CGI.pm before 3.63 for Perl does not properly escape newlines in Set-Cookie or P3P headers, allowing remote attackers to inject arbitrary headers into HTTP responses.
CVE-2012-6329	The Locale::Maketext implementation in Perl before 5.17.7 does not properly handle backslashes and method names, allowing context-dependent attackers to execute arbitrary commands via crafted translation strings.
CVE-2013-1667	The rehash mechanism in Perl 5.8.2 through 5.16.x allows context-dependent attackers to cause a denial of service (memory consumption and crash) via a crafted hash key.

CVE ID	Description
CVE-2013-7422	An integer underflow in the regular expression engine (regcomp.c) in Perl before 5.20 allows context-dependent attackers to execute arbitrary code or cause a denial of service via long digit strings.
CVE-2014-4330	The Dumper method in Data::Dumper before 2.154 allows context-dependent attackers to cause a denial of service (stack exhaustion and crash) via deeply nested Array-References.
CVE-2015-8853	The regular expression engine in Perl before 5.24.0 allows context-dependent attackers to cause a denial of service (infinite loop and high CPU usage) via crafted UTF-8 data.
CVE-2016-1238	Perl 5.x before 5.22.3 and 5.24.1 does not properly remove the current directory (".") from the module include path (@INC), allowing local users to gain privileges via a Trojan horse module.
CVE-2016-2381	Perl might allow context-dependent attackers to bypass the taint protection mechanism in a child process via duplicate environment variables in the envp array.
CVE-2016-6185	The XSLoader::load method in Perl does not properly locate shared object (.so) files when called in a string eval, potentially allowing local users to execute arbitrary code via a malicious library.
CVE-2018-12015	The Archive::Tar module in Perl through 5.26.2 allows remote attackers to bypass directory-traversal protection and overwrite arbitrary files via an archive containing a symlink and a regular file with the same name.
CVE-2018-18311	Perl before 5.26.3 and 5.28.1 has a buffer overflow vulnerability via a crafted regular expression that triggers invalid write operations.
CVE-2018-6913	A heap-based buffer overflow in the pack function in Perl before 5.26.2 allows context-dependent attackers to execute arbitrary code via a large item count.
CVE-2020-10543	Perl before 5.30.3 on 32-bit platforms allows a heap-based buffer overflow because nested regular expression quantifiers have an integer overflow.
CVE-2020-10878	Perl before 5.30.3 has an integer overflow related to mishandling of specific instructions in the regular expression engine, potentially leading to instruction injection.
CVE-2020-12723	A buffer overflow vulnerability in the regular expression compiler (regcomp.c) in Perl before 5.30.3 occurs during recursive calls to S_study_chunk.
CVE-2020-16156	CPAN 2.28 allows a signature verification bypass, which could allow an attacker to bypass security checks for Perl modules downloaded from the network.
CVE-2023-31484	CPAN.pm before 2.35 and Perl before 5.38.0 do not verify TLS certificates when downloading distributions over HTTPS, exposing users to man-in-the-middle attacks.

CVE ID	Description
CVE-2023-47038	A heap-based buffer overflow vulnerability was found in Perl 5.30.0 through 5.38.0 when compiling a crafted regular expression with illegal Unicode properties.
CVE-2024-56406	A heap buffer overflow vulnerability in Perl's tr operator occurs when processing non-ASCII bytes, potentially leading to a denial of service or arbitrary code execution.
CVE-2025-40909	A race condition in Perl threads during directory handle cloning can cause the current working directory to change unexpectedly, potentially allowing a local attacker to trick threads into loading malicious code.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.

Defect ID - CSCwr84274

This product includes third-party software that is affected by the vulnerabilities identified by the following Common Vulnerabilities and Exposures (CVE) IDs:

CVE ID	Description
CVE-2025-27363	An out-of-bounds write vulnerability in FreeType versions 2.13.0 and below occurs when parsing font subglyph structures in TrueType GX and variable font files; improper data type assignment leads to a buffer wraparound and undersized heap allocation, potentially allowing arbitrary code execution.

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.

Defect ID - CSCwr84317

This product includes third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerabilities and Exposures (CVE) IDs:

CVE ID	Description
CVE-2023-38545	A high-severity heap-based buffer overflow vulnerability in curl's SOCKS5 proxy handshake occurs when a host name longer than 255 bytes is incorrectly copied into a target buffer during a slow handshake, potentially allowing a malicious proxy to execute arbitrary code on the client.

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.

Defect ID - CSCwq11344

This product includes third-party software that is affected by the vulnerabilities identified by the following Common Vulnerabilities and Exposures (CVE) IDs:

CVE ID	Description
CVE-1999-0289	The Apache web server for Win32 may provide access to restricted files when a dot(.) is appended to a requested URL, potentially allowing unauthorized file disclosure.
CVE-1999-0678	A default configuration of Apache on Debian GNU/Linux sets the ServerRoot to/usr/doc, which allows remote users to read documentation files for the entire server.
CVE-2010-1151	A race condition in the mod_auth_shadow module for the Apache HTTP Server allows remote attackers to bypass authentication and read or modify data via improper interaction with an external helper application.
CVE-2023-31122	An out-of-bounds read vulnerability in the mod_macro module of Apache HTTP Server versions through 2.4.57 allows an attacker to cause a crash or obtain sensitive information when processing long macros.
CVE-2023-38709	Faulty input validation in the core of Apache HTTP Server through version 2.4.58 allows malicious or exploitable backend content generators to split HTTP responses, potentially leading to cache poisoning or XSS.
CVE-2023-43622	A flaw in the mod_http2 module allows an attacker opening an HTTP/2 connection with an initial window size of 0 to block handling of that connection indefinitely, exhausting worker resources in a "slow loris" style attack.
CVE-2023-45802	When an HTTP/2 stream is reset by a client, memory resources may not be reclaimed immediately, allowing a client to grow the server's memory footprint and potentially cause a denial of service.
CVE-2024-24795	An HTTP response splitting vulnerability in multiple Apache HTTP Server modules allows an attacker to inject malicious response headers into backend applications, leading to HTTP desynchronization attacks.
CVE-2024-27316	The Apache HTTP Server fails to limit the amount of HTTP/2 CONTINUATION frames sent within a single stream, which can lead to memory exhaustion and a denial of service condition.
CVE-2024-36387	Serving WebSocket protocol upgrades over an HTTP/2 connection in Apache HTTP Server could result in a null pointer dereference, leading to a crash of the server process.
CVE-2024-38472	A Server-Side Request Forgery (SSRF) vulnerability in Apache HTTP Server on Windows allows an attacker to potentially leak NTLM hashes to a malicious server via crafted requests or content.
CVE-2024-38473	An encoding problem in the mod_proxy module allows request URLs with incorrect encoding to be sent to backend services, potentially bypassing authentication via crafted requests.
CVE-2024-38474	A substitution encoding issue in mod_rewrite allows an attacker to execute scripts in directories permitted by configuration but not directly reachable by URL, or disclose script source code meant only for CGI execution.

CVE ID	Description
CVE-2024-38475	Improper escaping of output in mod_rewrite allows an attacker to map URLs to filesystem locations that are permitted to be served but are not intended to be directly reachable, potentially resulting in code execution.
CVE-2024-38476	Vulnerabilities in the core of Apache HTTP Server allow information disclosure, SSRF, or local script execution via backend applications whose response headers are malicious or exploitable.
CVE-2024-38477	A null pointer dereference in the mod_proxy module of Apache HTTP Server allows an attacker to crash the server via a specially crafted malicious request.
CVE-2024-39573	A potential SSRF vulnerability in mod_rewrite allows an attacker to cause unsafe RewriteRules to unexpectedly set up URLs to be handled by mod_proxy, bypassing intended access controls.
CVE-2024-40898	An SSRF vulnerability in Apache HTTP Server on Windows with mod_rewrite in server/vhost context allows potential leakage of NTLM hashes to a malicious server via crafted requests.
CVE-2025-3891	A flaw in the mod_auth_openidc module for Apache HTTP Server allows a remote attacker to trigger a denial of service by sending an empty POST request when the OIDCPreservePost directive is enabled.

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.

Defect ID - CSCws68830

This product includes third-party software that is affected by the vulnerabilities identified by the following Common Vulnerabilities and Exposures (CVE) IDs:

CVE ID	Description
CVE-2005-3962	An integer overflow in the format string functionality (Perl_sv_vcatpvfn) in Perl 5.8.6 and 5.9.2 allows attackers to overwrite arbitrary memory or execute arbitrary code via format string specifiers with large values.
CVE-2005-4278	An untrusted search path vulnerability in Perl before 5.8.7-r1 on Gentoo Linux allows local users in the portage group to gain privileges via a malicious shared object in the Portage temporary build directory.
CVE-2007-5116	A buffer overflow in the polymorphic opcode support in the Regular Expression Engine (regcomp.c) in Perl 5.8 allows context-dependent attackers to execute arbitrary code by switching from byte to Unicode characters in a regular expression.
CVE-2010-1158	An integer overflow in the regular expression engine in Perl 5.8.x allows context-dependent attackers to cause a denial of service (stack consumption and crash) by matching a crafted regular expression against a long string.

CVE ID	Description
CVE-2011-2728	The bsd_glob function in the File::Glob module for Perl before 5.14.2 allows context-dependent attackers to cause a denial of service (crash) via a glob expression with the GLOB_ALTDIRFUNC flag, triggering an uninitialized pointer dereference.
CVE-2011-2939	An off-by-one error in the decode_xs function in the Encode module for Perl allows context-dependent attackers to cause a denial of service (memory corruption) or execute arbitrary code via a crafted Unicode string.
CVE-2012-6329	The Locale::Maketext implementation in Perl before 5.17.7 does not properly handle backslashes and method names, allowing context-dependent attackers to execute arbitrary commands via crafted translation strings.
CVE-2013-1667	The rehash mechanism in Perl 5.8.2 through 5.16.x allows context-dependent attackers to cause a denial of service (memory consumption and crash) via a crafted hash key.
CVE-2014-4330	The Dumper method in Data::Dumper before 2.154 allows context-dependent attackers to cause a denial of service (stack exhaustion and crash) via deeply nested Array-References.
CVE-2015-8853	The regular expression engine in Perl before 5.24.0 allows context-dependent attackers to cause a denial of service (infinite loop and high CPU usage) via crafted UTF-8 data.
CVE-2016-1238	Perl 5.x before 5.22.3 and 5.24.1 does not properly remove the current directory (".") from the module include path (@INC), allowing local users to gain privileges via a Trojan horse module.
CVE-2016-2381	Perl might allow context-dependent attackers to bypass the taint protection mechanism in a child process via duplicate environment variables in the envp array.
CVE-2017-12814	A stack-based buffer overflow in the CPerlHost::Add method in win 32/perlhost.hin Perl before 5.24.3-RC1 and 5.26.x before 5.26.1-RC1 on Windows allows attackers to execute arbitrary code via a long environment variable.
CVE-2017-12837	A heap-based buffer overflow in the S_regatom function in regcomp.c in Perl before 5.24.3-RC1 and 5.26.x before 5.26.1-RC1 allows remote attackers to cause a denial of service via a regular expression with a \N{} escape and the case-insensitive modifier.
CVE-2017-12883	A buffer overflow in the S_grok_bslash_N function in regcomp.c in Perl before 5.24.3-RC1 and 5.26.x before 5.26.1-RC1 allows remote attackers to disclose sensitive information or cause a denial of service via a crafted regular expression with an invalid \N{U+...} escape.
CVE-2018-12015	The Archive::Tar module in Perl through 5.26.2 allows remote attackers to bypass directory-traversal protection and overwrite arbitrary files via an archive containing a symlink and a regular file with the same name.

CVE ID	Description
CVE-2018-18311	An integer overflow in the Perl_my_setenv function in Perl before 5.26.3 and 5.28.1 allows local attackers to cause a denial of service or execute arbitrary code via a large environment variable.
CVE-2018-18312	A heap-based buffer overflow in the S_handle_regex_sets function in regcomp.c in Perl before 5.26.3 and 5.28.1 allows remote attackers to cause a denial of service or execute arbitrary code via a crafted regular expression.
CVE-2018-18313	A heap-based buffer read overflow in the S_grok_bslash_N function in regcomp.c in Perl before 5.26.3 and 5.28.1 allows remote attackers to disclose sensitive information from process memory via a crafted regular expression.
CVE-2018-18314	A heap-based buffer overflow in the S_regatom function in regcomp.c in Perl before 5.26.3 and 5.28.1 allows remote attackers to cause a denial of service or execute arbitrary code via a crafted regular expression.
CVE-2018-6913	A heap-based buffer overflow in the pack function in Perl before 5.26.2 allows context-dependent attackers to execute arbitrary code via a large item count.
CVE-2020-10543	Perl before 5.30.3 on 32-bit platforms allows a heap-based buffer overflow because nested regular expression quantifiers have an integer overflow.
CVE-2020-10878	Perl before 5.30.3 has an integer overflow related to mishandling of specific instructions in the regular expression engine, potentially leading to instruction injection.
CVE-2020-12723	A buffer overflow vulnerability in the regular expression compiler (regcomp.c) in Perl before 5.30.3 occurs during recursive calls to S_study_chunk.
CVE-2022-48522	A stack-based crash (infinite recursion) in the S_find_uninit_var function in Perl 5.34.0 occurs when attempting to print warning messages, potentially leading to a denial of service.
CVE-2023-31484	CPAN.pm before 2.35 and Perl before 5.38.0 do not verify TLS certificates when downloading distributions over HTTPS, exposing users to man-in-the-middle attacks.
CVE-2023-31486	HTTP::Tiny before 0.083, a Perl core module, has an insecure default TLS configuration where users must opt in to verify certificates, potentially exposing applications to man-in-the-middle attacks.
CVE-2023-47039	A binary hijacking vulnerability in Perl for Windows occurs because it relies on the system path to find the shell (cmd.exe) and initially searches the current working directory, allowing local privilege escalation.

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 Cisco UCS XE-Series M8 Server Firmware Release, 6.0(1.260001) — None

Security fixes in Cisco UCS C-Series M8 6.0(1.250194) Server Firmware Release — None

Security fixes in Cisco UCS X-Series M8 6.0(1.252114), M7, M6 6.0(1.250179), B-Series M6, M5 6.0(1.250169), and C-Series M8, M7, M6 6.0(1.250192) Server Firmware Release — None

Security fixes in Cisco UCS XE-Series M8 6.0(1.251030) Server Firmware Release — None

Security fixes in Cisco UCS X-Series M8 6.0(1.252039) Server Firmware Release — None

Security fixes in Cisco UCS C-Series M8, M7, M6 6.0(1.250174) Server Firmware Release

This section provides a brief description of the security fixes.

Defect ID - CSCwq36167

The Cisco UCS C-Series M6 Rack Servers include an Intel CPU that is affected by the vulnerability identified by the following Common Vulnerability and Exposures (CVE) ID:

- **CVE-2025-20067** — Observable timing discrepancy in firmware for some Intel(R) CSME and Intel(R) SPS may allow a privileged user to potentially enable information disclosure via local access.

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.

Defect ID - CSCwq36171

The Cisco UCS C-Series M7 Rack Servers include an Intel CPU that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- **CVE-2025-21096** — Improper buffer restrictions in the firmware for some Intel(R) TDX may allow a privileged user to potentially enable escalation of privilege via local access.
- **CVE-2025-20053** — Improper buffer restrictions for some Intel(R) Xeon(R) Processor firmware with SGX enabled may allow a privileged user to potentially enable escalation of privilege via local access.
- **CVE-2025-24305** — Insufficient control flow management in the Alias Checking Trusted Module (ACTM) firmware for some Intel(R) Xeon(R) processors may allow a privileged user to potentially enable escalation of privilege via local access.
- **CVE-2025-20613** — Predictable Seed in Pseudo-Random Number Generator (PRNG) in the firmware for some Intel(R) TDX may allow an authenticated user to potentially enable information disclosure via local access.
- **CVE-2025-21090** — Missing reference to active allocated resource for some Intel(R) Xeon(R) processors may allow an authenticated user to potentially enable denial of service via local access.
- **CVE-2025-22853** — Improper synchronization in the firmware for some Intel(R) TDX may allow a privileged user to potentially enable escalation of privilege via local access.

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 Cisco UCS X-Series M8, M7, M6 6.0(1.250122), B-Series M6, M5 6.0(1.250127), and C-Series M8, M7, M6 6.0(1.250131) Server Firmware Release — None

Security fixes in Cisco UCS X-Series M8, M7, M6 6.0(1.250120), B-Series M6, M5 6.0(1.250126), and C-Series M8, M7, M6 6.0(1.250127) Server Firmware Release

This section provides a brief description of the security fixes.

Defect ID - CSCwm98102

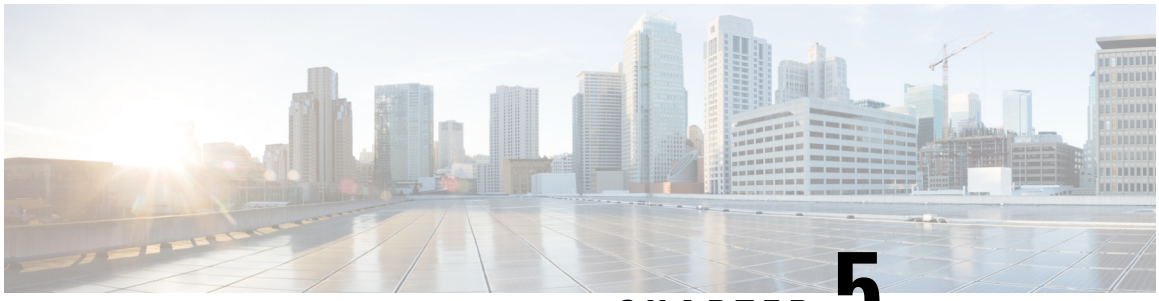
The Cisco products UCS B-Series Blade Servers, UCS C-Series Rack Servers and UCS X-Series Compute Nodes may include an optional Trusted Platform Module (TPM) 2.0 that is affected by the vulnerability identified by the following Common Vulnerability and Exposures (CVE) ID:

- **CVE-2025-2884** — TCG TPM2.0 Reference implementation's CryptHmacSign helper function is vulnerable to Out-of-Bounds read due to the lack of validation the signature scheme with the signature key's algorithm. See Errata Revision 1.83 and advisory TCGVRT0009 for TCG standard TPM2.0.

  Cisco UCS servers equipped with one of the following optional TPM modules:

- UCSX-TPM2-002
- UCSX-TPM-002C
- UCS-TPM-002D
- UCSX-TPM-002D

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.



CHAPTER 5

Resolved issues

You can view the open issues, resolved issues, and security fixes using the Cisco Bug Search Tool.

- Resolved issues in Cisco UCS C-Series C220 M8 and C240 M8 6.0(2.260236) Server Firmware Release, on page 46
- Resolved issues in Cisco UCS C-Series M8, M6 6.0(2.260205) Server Firmware Release, on page 46
- Resolved issues in Cisco UCS X-Series M8, M7 6.0(2.260180) and C-Series M8, M7 6.0(2.260180) Server Firmware Release — None, on page 48
- Resolved issues in Cisco UCS B-Series M5 6.0(1.260031) Server Firmware Release, on page 48
- Resolved issues in Cisco UCS X-Series M8, M7, M6 6.0(2.260143), XE-Series M8 6.0(2.260143), and C-Series M8, M7, M6 6.0(2.260143) Server Firmware Release, on page 49
- Resolved issues in Cisco UCS X-Series M8, M7 6.0(2.260069) and C-Series M8 6.0(2.260069) Server Firmware Release , on page 50
- Resolved issues in Cisco UCS B-Series M5 6.0(1.260012) Server Firmware Release, on page 52
- Resolved issues in Cisco UCS X-Series M8, M7, M6 6.0(2.260040), XE-Series M8 6.0(2.260042), C-Series M8, M7, M6 6.0(2.260044), and B-Series M6 6.0(2.260040) Server Firmware Release, on page 52
- Resolved issues in Cisco UCS XE-Series M8 Server Firmware Release, 6.0(1.260001), on page 56
- Resolved issues in Cisco UCS C-Series M8 6.0(1.250194) Server Firmware Release — None, on page 56
- Resolved issues in Cisco UCS X-Series M7 6.0(1.250179) and C-Series M7, M6 6.0(1.250192) Server Firmware Release, on page 56
- Resolved issues in Cisco UCS XE-Series M8 Server Firmware Release, 6.0(1.251030) — None, on page 57
- Resolved issues in Cisco UCS X-Series M8 6.0(1.252039) Server Firmware Release — None, on page 57
- Resolved issues in Cisco UCS X-Series M8 6.0(1.250162) and C-Series M8, M6 6.0(1.250174) Server Firmware Release, on page 57
- Resolved issues in Cisco UCS X-Series M8, M7, M6 6.0(1.250122), B-Series M6, M5 6.0(1.250127), and C-Series M8, M7, M6 6.0(1.250131) Server Firmware Release, on page 60
- Resolved issues in Cisco UCS C-Series M8, M7, and M6 6.0(1.250127) Server Firmware Release, on page 60

Resolved issues in Cisco UCS C-Series C220 M8 and C240 M8 6.0(2.260236) Server Firmware Release

This section provides a brief description of the resolved issues.

Defect ID	Description	First Version Affected	Resolved in Release
CSCww65328	On Cisco UCS C-Series C220 M8 and C240 M8 servers, the server may become unresponsive after multiple disk-related errors are reported. The operating system logs may repeatedly display the `Previous Firmware Lockup Detected` message. When this condition occurs, a hard reset is required to restore server operation. This issue is resolved.	4.3(6.250053)	6.0(2.260236)

Resolved issues in Cisco UCS C-Series M8, M6 6.0(2.260205) Server Firmware Release

This section provides a brief description of the resolved issues.

Defect ID	Description	First Version Affected	Resolved in Release
CSCwk74954	On Cisco UCS C245 M6 servers, if Cisco IMC crashes, the **IP Type** field in the Preboot Execution Environment (PXE) Boot configuration might change to **None** even though it is configured as **IPv4**. When this occurs, Intersight may show **Out of Sync** on the **Server Profile** > **Boot Order policy**. This issue is resolved.	4.2(3h)	6.0(2.260205)

Defect ID	Description	First Version Affected	Resolved in Release
CSCwv93860	On Cisco UCS C220 M8 servers in Intersight Standalone Mode, after a Redfish `PATCH` request is used to configure one-time Preboot Execution Environment (PXE) boot, the request may complete successfully but return the previous boot values in the response body. The boot setting is updated successfully, but the `PATCH` response body may not show the updated state. A follow-up `GET` request shows the correct PXE boot state. This issue is resolved.	4.3(2.260007)	6.0(2.260205)
CSCww03146	On Cisco UCS C225 M8 servers in Intersight Standalone Mode, a Redfish `PATCH` request for boot override settings may return a success response for invalid payloads. This condition can occur when an invalid enum value or an incorrect data type is sent for boot override fields. When this occurs, no error information may be returned, and the server state remains unchanged. This issue is resolved.	4.3(2.260007)	6.0(2.260205)
CSCwv66245 CSCwv82952	On Cisco UCS C-Series C245 M8 servers with AMD EPYC 9xx5 processors, the default **Auto** selection for the xGMI Link configuration was previously setting 3 xGMI links between processors instead of the intended 4 xGMI links. This issue has been resolved. The default **Auto** option now configures a 4xGMI link configuration. Additionally, BIOS token options are provided to revert to the previous configuration, along with the corresponding link speed selection. This change has no observable impact on the operating system environment.	4.3(6.250040)	6.0(2.260205)

Resolved issues in Cisco UCS X-Series M8, M7 6.0(2.260180) and C-Series M8, M7 6.0(2.260180) Server Firmware Release — None

Resolved issues in Cisco UCS B-Series M5 6.0(1.260031) Server Firmware Release

This section provides a brief description of the resolved issues.

Defect ID	Description	First Version Affected	Resolved in Release
CSCwn42410	A partial failure of one of the M.2 drives on a Cisco UCS-M2-HWRAID controller may cause the affected drive to be reported incorrectly and may degrade the RAID 1 virtual drive. In this condition, the drive can appear in `PhyDriveInfo` with no valid device data visible, while the reported link speed is reduced to 1.5 GB. Additional drive attributes such as power-on hours, power cycle count, percentage life, wear status days, and temperature may all appear as 0. Product ID and firmware fields may also be blank even though the drive is still shown as online. In some cases, the messages log may incorrectly report the affected drive as having 0% life remaining by generating an `SSD LIFE TIME LAPSE` fault. This issue has been observed on systems using the Cisco UCS-M2-HWRAID M.2 storage controller with M.2 drives configured in a RAID 1 virtual drive. This issue is resolved.	4.3(2.230207)	B-Series: 6.0(1.260031) C-Series M8, M7, M6 servers: 6.0(2.260143) C-Series M8, M7, M6 servers: 4.3(6.260054) C-Series: 4.3(2.260020)

Resolved issues in Cisco UCS X-Series M8, M7, M6 6.0(2.260143), XE-Series M8 6.0(2.260143), and C-Series M8, M7, M6 6.0(2.260143) Server Firmware Release

This section provides a brief description of the resolved issues.

Defect ID	Description	First Version Affected	Resolved in Release
CSCwt57564	On Cisco UCS X210c M8 servers with Cisco UCS Virtual Interface Card (VIC) adapters, VMware ESXi may display a Purple Screen of Death (PSOD) with a Peripheral Component Interconnect (PCI) bus error. The error message may indicate an undiagnosed PCI bus error and an event received for a port with no Downstream Port Containment (DPC) driver. This issue occurs when the posted value in the ring registers does not increment as expected, preventing the software from detecting that an indirect transaction has arrived. This issue is resolved.	X-Series M8 (X215c): 5.3(0.240016) X-Series M8 (X210c): 5.4(0.250037) X-Series M8 (X410c): 6.0(2.260040)	X-Series M8 (X410c, X215c, X210c): 6.0(2.260143) X-Series M8 (X215c, X210c): 5.4(0.260044), 5.4(0.260049)
CSCwt65289	On Cisco UCS C-Series, X-Series, or XE-Series servers with Non-Volatile Memory Express (NVMe) drives, Fault History may report `NVMe disk inoperable` events during a host firmware upgrade. In this condition, the firmware upgrade completes successfully, and the reported messages are cleared after the host reboots following the firmware update process. The drive inoperable messages can be safely ignored during the host firmware upgrade. This issue is resolved.	6.0(2.260044)	X-Series: 6.0(2.260143) XE-Series: 6.0(2.260143) C-Series: 6.0(2.260143)
CSCwt73073	On Cisco UCS X210c M7 servers, after a Basic Input/Output System (BIOS) upgrade to release 6.0(2.260040), an inventory fault may be reported for an unknown Peripheral Component Interconnect Express (PCIe) card on a riser. When this condition occurs, the adapter on the affected riser may not be detected after the upgrade. This issue is resolved.	6.0(2.260040)	X-Series: 6.0(2.260143)

Defect ID	Description	First Version Affected	Resolved in Release
CSCwn42410	A partial failure of one of the M.2 drives on a Cisco UCS-M2-HWRAID controller may cause the affected drive to be reported incorrectly and may degrade the RAID 1 virtual drive. In this condition, the drive can appear in `PhyDriveInfo` with no valid device data visible, while the reported link speed is reduced to 1.5 GB. Additional drive attributes such as power-on hours, power cycle count, percentage life, wear status days, and temperature may all appear as 0. Product ID and firmware fields may also be blank even though the drive is still shown as online. In some cases, the messages log may incorrectly report the affected drive as having 0% life remaining by generating an `SSD LIFE TIME LAPSE` fault. This issue has been observed on systems using the Cisco UCS-M2-HWRAID M.2 storage controller with M.2 drives configured in a RAID 1 virtual drive. This issue is resolved.	4.3(2.230207)	C-Series: 6.0(2.260143), 4.3(6.260054)

Resolved issues in Cisco UCS X-Series M8, M7 6.0(2.260069) and C-Series M8 6.0(2.260069) Server Firmware Release

This section provides a brief description of the resolved issues.

Defect ID	Description	First Version Affected	Resolved in Release
CSCwt34870	Cisco UCS C-series servers running firmware version 6.0.2.260044 may experience Simple Network Management Protocol (SNMP) service becoming unresponsive when performing `snmpget` operations on private enterprise OIDs, subsequently causing `snmpwalk` requests to fail. If the service becomes unresponsive, it can be restored by rebooting the Baseboard Management Controller (BMC) or by disabling and re-enabling the SNMP service. This issue is resolved.	C-Series: 6.0(2.260044)	C-Series: 6.0(2.260069)
CSCwt18924	After an upstream Cisco ACI fabric upgrade or reload, Cisco UCS VIC adapters may fail to bring vNICs online. The adapter physical interfaces come up, but the vNICs remain stuck in an initializing state and do not recover automatically. Adapter logs may show the adapter encountering out-of-memory conditions, followed by a reset. This issue is observed with 10GBase-T (10G-T-X) transceivers on Cisco UCS VIC 1400 Series and 15000 Series adapters and may be triggered during switch or server reload events when the transceiver holds the I2C bus, leading to a memory leak in the adapter. This issue is resolved.	C-Series: 4.3(5.250030)	C-Series: 6.0(2.260069)
CSCwt42347	During the Host Firmware Package (HFP) upgrade from release 4.3(2) to 6.0(2), Cisco UCS X-Series servers with UCSX-X10C-RAIDF controller experience failure at the stage `Preparing to check hardware configuration` causing the Unified BIOS Management (UBM) upgrade to hang. The firmware update process does not complete, and BMC logs show the update process running indefinitely. This issue is resolved.	X-Series: 6.0(2.260040)	X-Series: 6.0(2.260069)

Defect ID	Description	First Version Affected	Resolved in Release
CSCwt35920	Firmware updates may fail on certain RTX Pro 6000 GPUs shipped as spares, leaving them at an older firmware version. This issue is limited to specific spare units and does not affect the overall update process. This issue is resolved.	X-series: 6.0(2.260040) C-series: 6.0(2.260044) X580p PCIe Node: 6.0(2.260043)	X-Series: 6.0(2.260069) C-Series: 6.0(2.260069) X580p PCIe Node: 6.0(2.260069)

Resolved issues in Cisco UCS B-Series M5 6.0(1.260012) Server Firmware Release

This section provides a brief description of the resolved issues.

Defect ID	Description	First Version Affected	Resolved in Release
CSCwr21671	On Cisco UCS B200 M5 servers with an LSI 12G RAID controller running Windows Server 2019 (megasas2 driver), an L2/L3 cache error may be detected on the RAID controller. This causes the storage controller to become inoperable, and Cisco IMC is unable to detect the controller. This issue is resolved.	4.2(3e)	5.4(0.260011) 6.0(1.260012)

Resolved issues in Cisco UCS X-Series M8, M7, M6 6.0(2.260040), XE-Series M8 6.0(2.260042), C-Series M8, M7, M6 6.0(2.260044), and B-Series M6 6.0(2.260040) Server Firmware Release

This section provides a brief description of the resolved issues.

Defect ID	Description	First Version Affected	Resolved in Release
CSCws30219	Cisco UCS M7 servers may experience host lockups due to ECC errors during runtime. The BIOS fails to retrieve a variable properly, causing EFI to return an invalid parameter, which leads to the host freezing without any logs or Cisco IMC alerts.The host becomes unresponsive, and KVM input is not accepted. This issue is resolved.	X-Series M7: 5.4(0.250048) C-series M7: 4.3(6.250053)	X-Series M7: 6.0(2.260040) C-Series M7: 6.0(2.260044)
CSCws62117	Cisco UCS C240-M8 server with LPe35002-M2 Emulex adapters connected to Brocade SAN switches and Dell storage arrays experience intermittent I_T NexusLoss errors, causing unstable connections and periodic LUN disconnections. Although FCP I/O completes without errors, the adapter repeatedly attempts to re-establish the connection by issuing LOGO and FLOGI commands, which temporarily restore connectivity before the issue recurs. This issue is resolved.	4.3(6.250053)	6.0(2.260044)
CSCwr51315	On Cisco UCS X-series servers, NVMe drives UCS-NVMEG4-M7680 with firmware E2CS005 show an SSID of 5000 instead of the expected Cisco SSID 4800. This discrepancy causes compliance checks to fail, marking the disks as unclaimed. This issue is resolved.	6.0(1.250120)	6.0(2.260040)
CSCwr73352	Multiple Cisco UCS x210C M7 servers experience Cisco IMC reboots triggered by BMC watchdog hard resets. This causes service profiles to become inaccessible temporarily during the reboot. This behavior may impact server management availability during the reset events. This issue is resolved.	5.2(1.240010)	6.0(2.260040)

Defect ID	Description	First Version Affected	Resolved in Release
CSCwq55604	DIMM_P2_H1 on all Cisco UCS C245 M8 integrated servers reports as inoperable, although all DIMMs function correctly with no memory errors. The issue triggers alerts indicating equipment inoperability and incompatible server firmware, despite the server being fully populated with supported identical DIMM models. This issue is resolved.	4.3(5.250001)	6.0(2.260044)
CSCwq17020	After installing U3 Micron drives with capacities of 3.8TB or larger in JBOD mode behind the UCSX-X10C-RAIDF controller, Linux OS fails to boot due to BIOSerrors related to loading the EFI boot image. This issue occurs specifically on Cisco UCS X-Series M8 servers equipped with Intel® processors and affects multiple Linux distributions. The problem does not occur when the drives are configured in RAID 0. Microsoft Windows® and Linux OS boot successfully on smaller capacity drives or when using RAID 0. This issue is resolved.	X210c: 5.4(0.250037) X215c: 5.4(0.250035)	6.0(2.260040)
CSCwr82017	On Cisco UCS X210c M8, C220 M8, and C240 M8 servers, the system continuously reboots if you enable IntelSGX and set the Processor Reserved Memory Range Registers (PRMRR) size to an unsupported value in the system memory settings. This issue occurs only when an unsupported PRMRR size is configured. This issue is resolved.	X-Series M8: 6.0(1.252114) C-series M8: 6.0(1.250192)	X-Series M8: 6.0(2.260040) C-series M8: 6.0(2.260044)

Defect ID	Description	First Version Affected	Resolved in Release
CSCwr82475	On Cisco Unified Edge servers UCSXE-130C-M8, after upgrading from firmware version 6.0(1.250003) to 6.0(1.251026) in UEFI-Secure boot mode, BMC boot may fail to transfer FIT4 records to the Secondary Service Processor (SSP) due to timing and race conditions. This prevents the required authentication handshake, causing the host system's POST to hang. You will see a **BIOS POST completion failed** error, and log messages such as: • peci command(0xa1) failed: 0x63 • peci rdpkgconfig command (0xa1) failed (result code: 0x63, addr: 0x30) • ast2600-ssp ahb:secondary-service-processor: Kicking SSP vqid = 1 **Workaround**: Reboot the BMC to resolve the issue.	XE-Series M8: 6.0(1.250003)	XE-Series M8: 6.0(2.260042)
CSCwr05911	On Cisco Unified Edge servers, when the host is powered off, the IMM Inventory page displays the LOM-NIC-1 interfaces as up on eCMC:A, but asdownon eCMC:B. This inconsistency occurs only when the host is powered off. There is no functional impact due to this issue. This issue is resolved.	XE-Series M8: 6.0(1.251030)	XE-Series M8: 6.0(2.260042)
CSCwr45526	Certain Cisco UCS servers experience boot interruptions caused by validation failures in the Secure Boot database. This issue affects specific server models during system startup, leading to potential boot interruptions and impacting system reliability. The problem arises from outdated certificates in the Secure Boot database that prevent successful secure boot processes. This issue is resolved.	C-series: 4.3(6.260017) B-series: 5.4(0.260011)	C-series: 6.0(2.260044) B-series: 6.0(2.260040)

Resolved issues in Cisco UCS XE-Series M8 Server Firmware Release, 6.0(1.260001)

This section provides a brief description of the resolved issues.

Defect ID	Description	First Version Affected	Resolved in Release
CSCws24234	On Cisco UCS XE130c M8 Compute Node, when the UCS-M2-HWRAID2 MINI STOR controller is missing but its carrier is installed, the system log is continuously flooded with `unable to read fru information` errors. Upgrade the firmware to resolve this issue. If the same errors persist post-upgrade, physically verify that both the M.2 controller and its carrier are properly seated and installed.	6.0(1.251030)	6.0(1.260001)
CSCws22743	On Cisco UCS XE130c servers, L4/L40S GPUs may experience a link downgrade to x8 width and GEN 1 speed due to a race condition. This can reduce GPU performance and typically occurs when the link is downgraded or lane width is reduced. To recover from a link downgrade, a workaround has been implemented to return the device to normal operation.	6.0(2.250123)	6.0(1.260001)

Resolved issues in Cisco UCS C-Series M8 6.0(1.250194) Server Firmware Release — None

Resolved issues in Cisco UCS X-Series M7 6.0(1.250179) and C-Series M7, M6 6.0(1.250192) Server Firmware Release

This section provides a brief description of the resolved issues.

Defect ID	Description	First Version Affected	Resolved in Release
CSCws30219	Cisco UCS M7 servers are susceptible to host lockups triggered by ECC (Error Correcting Code) memory events. This issue is specifically related to how the server's BIOS interacts with the EFI (Extensible Firmware Interface) during error conditions. During these events, the BIOS does not correctly retrieve a required variable, causing EFI to return an invalid parameter. As a result, the operating system is unable to continue normal operation and freezes without logging any errors. When this occurs, the host becomes unresponsive and KVM (keyboard, video, mouse) input is not accepted. Single-bit ECC errors—while not logged due to DDR5 specifications—can trigger this condition, resulting in complete loss of host responsiveness.	X-Series M7: 5.4(0.250048) C-series M7: 4.3(6.250053)	X-Series M7: 6.0(1.250179) C-series M7: 6.0(1.250192)
CSCwi71153	On Cisco UCS C-Series M6 servers, BMC reset occurs due to watchdog reset caused by kernel scheduler null pointer dereference. In addition, kernel panic might also occur in the server.	4.2(3b)	C-Series M6: 6.0(1.250192)

Resolved issues in Cisco UCS XE-Series M8 Server Firmware Release, 6.0(1.251030) — None

Resolved issues in Cisco UCS X-Series M8 6.0(1.252039) Server Firmware Release — None

Resolved issues in Cisco UCS X-Series M8 6.0(1.250162) and C-Series M8, M6 6.0(1.250174) Server Firmware Release

This section provides a brief description of the resolved issues.

Defect ID	Description	First Version Affected	Resolved in Release
CSCwq61388	On Cisco UCS C-Series M6 servers running CIMC 4.3.5 or later, enabling VMD in BIOS with multiple NVMe drives can cause storage subsystem initialization to exceed 15 minutes, leading to Intersight Server Profile deployment failures. The likelihood of encountering this issue increases with the number of drives installed. Disabling VMD or reducing the number of drives can resolve the issue.	4.3(5.250001)	6.0(1.250162) 6.0(1.250174)
CSCwq74490	On the Cisco UCS C245 M8 platform with AMD EPYC 9655 processors, fully loaded NVIDIA L4 GPUs experience random PCIe link width downgrades on different slots when running the Linux Rebooter Stress test. The affected slots change after actions such as an AC power cycle or HUU update; for example, if slots 2 and 6 are downgraded initially, other slots may be downgraded after these actions. This results in GPUs operating at reduced speeds in the OS environment.	4.3(6.250053)	6.0(1.250162) 6.0(1.250174)
CSCwq01863	On Cisco UCS C225 or C245 M8 servers in standalone mode, configuring secure LDAP (LDAPS) on any port other than 636 results in the server attempting a standard LDAP connection instead of a secure one, causing LDAPS authentication to fail. Always use port 636 for secure LDAP connections. Other ports will not work for LDAPS.	4.3(6.250044)	6.0(1.250162) 6.0(1.250174)

Defect ID	Description	First Version Affected	Resolved in Release
CSCwr24516	On Cisco UCS X210c M8, some servers may not power on or start up if they contain a hardware part (inductor) from a specific vendor. This issue causes a startup failure, and the server will remain off even when you try to turn it on. The problem is caused by a difference in how the new hardware part works, but it can be fully resolved by updating the board to the latest VR (Voltage Regulator) image, which is designed to support this new component. Update the server with the latest VR image, clear any power on error, and turn the server off and on again. If the server still does not start, contact Cisco TAC for further assistance.	6.0(1.250126)	6.0(1.250162) 6.0(1.250174)
CSCwp91696	On Cisco UCS X215c M8 servers, when an E3.S NVMe drive is added to an empty slot while the server is already running, the drive connects at Gen 4 speed instead of Gen 5. This issue only occurs if the slot was empty during boot and the drive is hot inserted after the operating system has started. Insert the drive into the slot before powering on the server. Drives added later will only operate at Gen 4 speed until the server is rebooted.	6.0(1.250065)	6.0(1.250162) 6.0(1.250174)
CSCwq01510	On Cisco UCS X215c-M8servers, hot plugging E3.S NVMe drives in slot 8 or slot 9 does not work in ESXi or Windows if those slots were empty when the operating system started. Drives added or removed after boot are not detected by the OS. There is no workaround. Hot plugging in slots 8 and 9 will not function if the slots are empty during OS boot.	6.0(1.250086)	6.0(1.250162) 6.0(1.250174)

Defect ID	Description	First Version Affected	Resolved in Release
CSCwq93635	On Cisco UCS C240 M6 servers running CIMC 4.3.5 and later firmware, deployments with a large number of NVMe drives and VMD enabled in the BIOS may experience prolonged storage subsystem initialization times, taking up to 50 minutes. This delay can cause the **Wait for storage subsystem initialization** task to fail in Intersight Server Profile workflows, especially after the **Wait for BIOS POST Completion** step. If possible, turn off VMD in the BIOS to avoid the delay. If VMD must stay on, try using fewer NVMe drives during the initial setup, since the more drives you have, the longer the initialization takes.	4.3(6.250077)	6.0(1.250162) 6.0(1.250174)

Resolved issues in Cisco UCS X-Series M8, M7, M6 6.0(1.250122), B-Series M6, M5 6.0(1.250127), and C-Series M8, M7, M6 6.0(1.250131) Server Firmware Release

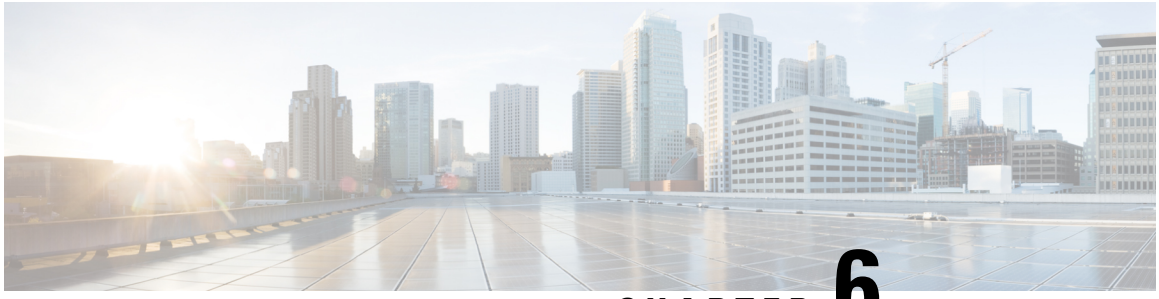
This section provides a brief description of the resolved issues.

Defect ID	Description	First Version Affected	Resolved in Release
CSCwq58890	The firmware for the Cisco UCS VIC 15000 series adapters is updated to fix a rare, intermittently seen memory issue and to ensure more robust and consistent operation across diverse memory types and configurations. **Note** If you continue to experience any memory error, then contact Cisco TAC.	X-series: 6.0(1.250120) B-series: 6.0(1.250126) C-series: 6.0(1.250127)	X-series: 6.0(1.250122) B-series: 6.0(1.250127) C-series: 6.0(1.250131)

Resolved issues in Cisco UCS C-Series M8, M7, and M6 6.0(1.250127) Server Firmware Release

This section provides a brief description of the resolved issues.

Defect ID	Description	First Version Affected	Resolved in Release
CSCwn99720	On Cisco UCS C-Series M8 servers with Intel processors and an R1S CPU configured in a single-CPU setup on the 2-socket platform, Intel SGX remains disabled even after being enabled in the BIOS. This issue does not occur with a dual CPU configuration.	4.3(6.250039)	6.0(1.250127) 4.3(6.250044)



CHAPTER 6

Open issues

You can view the open issues, resolved issues, and security fixes using the Cisco Bug Search Tool.

- Open issues in Cisco UCS C-Series C220 M8 and C240 M8 6.0(2.260236) Server Firmware Release — None, on page 64
- Open issues in Cisco UCS X-Series M8, M7, M6 6.0(2.260205), C-Series M8, M7, M6 6.0(2.260205), and B-Series M6 6.0(2.260205) Server Firmware Release — None, on page 64
- Open issues in Cisco UCS X-Series M8, M7 6.0(2.260180) and C-Series M8, M7 6.0(2.260180) Server Firmware Release — None, on page 64
- Open issues in Cisco UCS B-Series M5 6.0(1.260031) Server Firmware Release — None, on page 64
- Open issues in Cisco UCS X-Series M8 6.0(2.260143) Server Firmware Release, on page 64
- Open issues in Cisco UCS X-Series M8, M7, M6 6.0(2.260069), C-Series M8, M7, M6 6.0(2.260069), and B-Series M6 6.0(2.260069) Server Firmware Release, on page 65
- Open issues in Cisco UCS B-Series M5 6.0(1.260012) Server Firmware Release — None, on page 65
- Open issues in Cisco UCS X-Series M8, M7, M6 6.0(2.260040), XE-Series M8 6.0(2.260042), C-Series M8, M7, M6 6.0(2.260044), and B-Series M6 6.0(2.260040) Server Firmware Release, on page 65
- Open issues in Cisco UCS XE-Series M8 Server Firmware Release, 6.0(1.260001) — None, on page 68
- Open issues in Cisco UCS C-Series M8 6.0(1.250194) Server Firmware Release — None, on page 68
- Open issues in Cisco UCS X-Series M8 6.0(1.252114) and C-Series M8 6.0(1.250192) Server Firmware Release, on page 68
- Open issues in Cisco UCS XE-Series M8 Server Firmware Release, 6.0(1.251030), on page 68
- Open issues in Cisco UCS X-Series M8 6.0(1.252039) Server Firmware Release — None, on page 71
- Open issues in Cisco UCS X-Series M8, M7, M6 6.0(1.250162), B-Series M6, M5 6.0(1.250157), and C-Series M8, M7, M6 6.0(1.250174) Server Firmware Release — None, on page 71
- Open issues in Cisco UCS X-Series M8, M7, M6 6.0(1.250122), B-Series M6, M5 6.0(1.250127), and C-Series M8, M7, M6 6.0(1.250131) Server Firmware Release — None, on page 71
- Open issues in Cisco UCS X-Series M8, M7, M6 6.0(1.250120), B-Series M6, M5 6.0(1.250126), and C-Series M8, M7, M6 6.0(1.250127) Server Firmware Release, on page 71

Open issues in Cisco UCS C-Series C220 M8 and C240 M8 6.0(2.260236) Server Firmware Release — None

Open issues in Cisco UCS X-Series M8, M7, M6 6.0(2.260205), C-Series M8, M7, M6 6.0(2.260205), and B-Series M6 6.0(2.260205) Server Firmware Release — None

Open issues in Cisco UCS X-Series M8, M7 6.0(2.260180) and C-Series M8, M7 6.0(2.260180) Server Firmware Release — None

Open issues in Cisco UCS B-Series M5 6.0(1.260031) Server Firmware Release — None

Open issues in Cisco UCS X-Series M8 6.0(2.260143) Server Firmware Release

This section provides a brief description of the open issues.

Defect ID	Description	Workaround	First Version Affected
CSCwu59180	On Cisco UCS X215c M8 servers with an L40S Graphics Processing Unit (GPU), when used with the X580p PCIe node, the GPU lane width may downgrade from x16 to x8 after a system reboot. This issue occurs rarely and is not seen on every reboot. When this condition occurs, system performance may be affected.	Use the `lspci` command to check the lane width and reboot the Cisco UCS X215c M8 server if the lane width is degraded.	6.0(2.260069)

Open issues in Cisco UCS X-Series M8, M7, M6 6.0(2.260069), C-Series M8, M7, M6 6.0(2.260069), and B-Series M6 6.0(2.260069) Server Firmware Release

This section provides a brief description of the open issues.

Defect ID	Description	Workaround	First Version Affected
CSCws49799	On Cisco UCS C-Series servers, drives may be incorrectly reported as **Degraded** in the Out-of-Band (OOB) interface after hot-plugging during Virtual Machine (VM) operations on ESXi 9. This issue occurs because the system fails to properly process specific NVMe-MI command responses, leading to inaccurate performance metrics and persistent, false health alerts that do not clear even after physical drive reseating.	There is no direct workaround for this issue. The problem is being addressed through code improvements that enhance how the system handles device response.	C-Series: 6.0(2.260068)

Open issues in Cisco UCS B-Series M5 6.0(1.260012) Server Firmware Release — None

Open issues in Cisco UCS X-Series M8, M7, M6 6.0(2.260040), XE-Series M8 6.0(2.260042), C-Series M8, M7, M6 6.0(2.260044), and B-Series M6 6.0(2.260040) Server Firmware Release

This section provides a brief description of the open issues.

Defect ID	Description	Workaround	First Version Affected
CSCwt18924	On Cisco UCS C220 M6 servers with VIC 1467 adapters, a fatal crash due to out-of-memory errors occurs when upstream ACI switches are upgraded and rebooted. Physical ports show as up, but vNICs remain stuck in initializing and do not recover automatically. Adapter logs indicate resets from fatal errors.	Reboot the server to restore vNIC connectivity.	4.3(5.250030)

Defect ID	Description	Workaround	First Version Affected
CSCwt34436	On Cisco Unified Edge servers (UCSXE-130C-M8-20, UCSXE-130C-M8-32), the server discovery workflow fails at the `Wait for Server Inventory Completion` task. This issue occurs after upgrading Unified Edge and causes the Server Discovery workflow to halt at the `Inventory Collection` task, affecting 3 out of 4 servers.	Manually initiate a 'Rediscover' on individual servers to complete server discovery successfully.	6.0(2.260042)
CSCws19521	The downgrade of the server firmware to any release earlier than 6.0(2.260040) for Cisco UCS x210C M8 server equipped with UCSX-X10C-PT4F controller fails due to a Complex Programmable Logic Device (CPLD) firmware version mismatch.	Exclude the CPLD component from the HFP.	6.0(2.260040)
CSCwt42347	During the Host Firmware Package (HFP) upgrade from release 4.3(2) to 6.0(2), Cisco UCS X-Series servers with UCSX-X10C-RAIDF controller experience failure at the stage `Preparing to check hardware configuration` causing the Unified BIOS Management (UBM) upgrade to hang. The firmware update process does not complete, and BMC logs show the update process running indefinitely.	There is no known workaround. This issue occurs when a UBM firmware update is needed. The UBM component affects only the UCSX-X10C-RAIDF controller and does not impact other mezzanine cards that include UBM parts.	6.0(2.260040)

Defect ID	Description	Workaround	First Version Affected
CSCwt41941	On Cisco UCS C220 and C240 M8 servers, firmware versions using Intel Secondary Service Processor (SSP) 2.0 are not backward compatible with earlier releases using SSP 1.6. The firmware versions that support SSP 2.0 are: 4.3(6.260003), 6.0(1.250192), and 6.0(2.260044) or later. Downgrading to an earlier version causes the Baseboard Management Controller (BMC) to fail BIOS attestation, leading to critical system instability. Symptoms include systems getting stuck in the KVM console, boot failures, POST hangs, Catastrophic Error (CATERR) events, inoperable NVMe devices, and temperature sensor failures along with critical thermal threshold errors.	If you downgrade to an earlier firmware version and BMC fails, use the following recovery steps: **1.** Upgrade BMC Firmware: Use the Host Software Upgrade (HSU) or the Cisco IMC interface to upgrade only the BMC firmware component to the latest version (SSP 2.0 compatible). **2.** Perform a Host Power Reset: A full host power reset may help recover the system state, though it is not guaranteed to be 100% effective in all scenarios.	6.0(2.260044) 6.0(1.250192) 4.3(6.260003)
CSCwt35920	Firmware updates may fail on certain RTX Pro 6000 GPUs shipped as spares, leaving them at an older firmware version. This issue is limited to specific spare units and does not affect the overall update process.	There is no known workaround.	X-series: 6.0(2.260040) XE-series: 6.0(2.260042) C-series: 6.0(2.260044) B-series: 6.0(2.260040)

Open issues in Cisco UCS XE-Series M8 Server Firmware Release, 6.0(1.260001) — None

Open issues in Cisco UCS C-Series M8 6.0(1.250194) Server Firmware Release — None

Open issues in Cisco UCS X-Series M8 6.0(1.252114) and C-Series M8 6.0(1.250192) Server Firmware Release

This section provides a brief description of the open issues.

Defect ID	Description	Workaround	First Version Affected
CSCwr82017	On Cisco UCS X210c M8, C220 M8, and C240 M8 servers, the system continuously reboots if you enable Intel SGX and set the PRMRR size to an unsupported value in the system memory settings. This issue occurs only when an unsupported PRMRR size is configured.	When enabling Intel SGX, make sure to configure the PRMRR size to a supported value.	X-Series M8: 6.0(1.252114) C-series M8: 6.0(1.250192)

Open issues in Cisco UCS XE-Series M8 Server Firmware Release, 6.0(1.251030)

This section provides a brief description of the open issues.

Defect ID	Description	Workaround	First Version Affected
CSCwr05911	On Cisco Unified Edge servers, when the host is powered off, the IMM Inventory page displays the LOM-NIC-1 interfaces as **up** on eCMC:A, but as **down** on eCMC:B. This inconsistency occurs only when the host is powered off. There is no functional impact due to this issue.	There is no known workaround.	6.0(1.251030)
CSCwr63339	On Cisco Unified Edge servers, if the chassis enters an insufficient power state during runtime (after the node's BMC has already booted), you can still power on the CPU using the physical power button on the front panel. This may cause the BMC to become unstable for that node, as indicated by specific logs/events. The issue does not occur if the chassis is already in a power-deprived state before the server boots.	Remove the node that is causing high power usage, or upgrade to a power supply unit (PSU) with higher wattage to provide enough power.	6.0(1.251030)
CSCwr88145	On Cisco UCS XE M8 servers, the 2x10G front port (FP) LEDs remain ON even after the network cable is unplugged, if the port speed is set to 1 Gbps. The LED only turns off after a full server power cycle.	Restart the server to turn off the LED after unplugging the cable from the 1 Gbps port.	6.0(1.251030)

Defect ID	Description	Workaround	First Version Affected
CSCwr04128	On Cisco Unified Edge servers, server discovery intermittently fails in the Intersight workflow with the error message: "Adapter model CPUIntegratedNIC is not supported." This issue occurs occasionally and does not affect every discovery attempt.	To resolve, re-initiate the discovery process when this error appears.	6.0(1.251030)
CSCwq72323	The Compute Sled may fail to power off due to a very rare internal CPU issue. During the power off process, the CPU does not set SLP4_N and SLP3_N signals low, preventing the system from powering down. Manual power operations via IMM may return errors such as **Failed to set host power** or **Timer expired**. The issue persists until the next AC cycle.	To restore normal operation, perform an AC cycle of the Compute Sled: **1.** Log in to Intersight. **2.** Navigate to **Unified Edge** > **Unified Edge Chassis** **3.** Open the **Actions** drop-down menu on the right **4.** Click **Power Cycle Unified Edge Slot**, enter the server slot number, and press the Power Cycle button The system will become operational after a few minutes.	6.0(1.251030)

Open issues in Cisco UCS X-Series M8 6.0(1.252039) Server Firmware Release — None

Open issues in Cisco UCS X-Series M8, M7, M6 6.0(1.250162), B-Series M6, M5 6.0(1.250157), and C-Series M8, M7, M6 6.0(1.250174) Server Firmware Release — None

Open issues in Cisco UCS X-Series M8, M7, M6 6.0(1.250122), B-Series M6, M5 6.0(1.250127), and C-Series M8, M7, M6 6.0(1.250131) Server Firmware Release — None

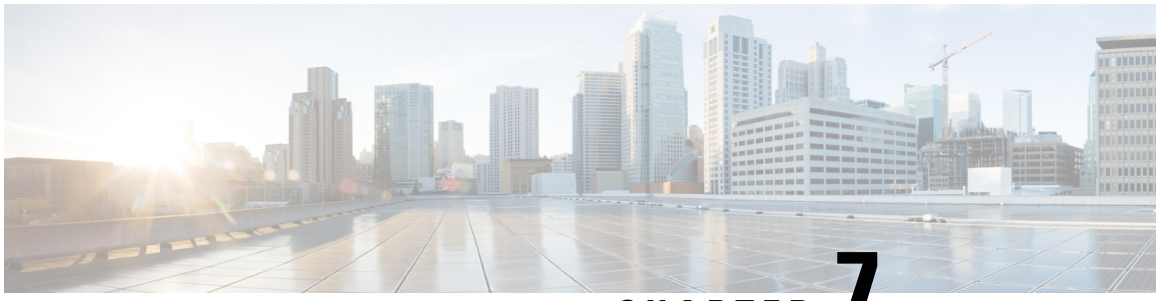
Open issues in Cisco UCS X-Series M8, M7, M6 6.0(1.250120), B-Series M6, M5 6.0(1.250126), and C-Series M8, M7, M6 6.0(1.250127) Server Firmware Release

This section provides a brief description of the open issues.

Defect ID	Description	Workaround	First Version Affected
CSCws30219	Cisco UCS M7 servers are susceptible to host lockups triggered by ECC (Error Correcting Code) memory events. This issue is specifically related to how the server's BIOS interacts with the EFI (Extensible Firmware Interface) during error conditions. During these events, the BIOS does not correctly retrieve a required variable, causing EFI to return an invalid parameter. As a result, the operating system is unable to continue normal operation and freezes without logging any errors. When this occurs, the host becomes unresponsive and KVM (keyboard, video, mouse) input is not accepted. Single-bit ECC errors—while not logged due to DDR5 specifications—can trigger this condition, resulting in complete loss of host responsiveness.	Downgrade server bundle: • For X-Series servers, downgrade the server bundle to version 5.4(0.250040) or an earlier release. • For C-Series servers, downgrade the server bundle to version 4.3(6.250044) or an earlier release.	X-Series M7: 5.4(0.250048) C-series M7: 4.3(6.250053)

Defect ID	Description	Workaround	First Version Affected
CSCwq61388	On Cisco UCS C-Series M6 servers running CIMC 4.3.5 or later, enabling VMD in BIOS with multiple NVME drives can cause storage subsystem initialization to exceed 15 minutes, leading to Intersight Server Profile deployment failures. Disabling VMD or reducing the number of drives can resolve the issue. Earlier firmware versions may not be affected.	• If VMD is not needed, disable it. • If disabling VMD is not possible, use the minimum number of NVME drives for setup, as more drives slow down system startup.	4.3(5.250001)
CSCwm33093	On Microchip-based storage cards, the Virtual Drive (VD) shows as "Inoperable" even when all disks are online because the firmware automatically changes drive assignments to optimize performance, ignoring user settings from management tools.	Use arcconf output to check drive assignments in spans. Firmware may override management tool settings for better performance.	4.3(5.240134)

Defect ID	Description	Workaround	First Version Affected
CSCwq17020	After installing U3 Micron drives with capacities of 3.8TB or larger in JBOD mode behind the UCSX-X10C-RAIDF controller, Linux OS fails to boot due to BIOS errors related to loading the EFI boot image. This issue occurs specifically on Cisco UCS X-Series M8 servers equipped with Intel® processors and affects multiple Linux distributions. The problem does notoccur when the drives are configured in RAID 0.Microsoft Windows® and Linux OS boot successfully on smaller capacity drives or when using RAID 0.	Install the OS on drive configured in RAID.	X210c: 5.4(0.250037) X215c: 5.4(0.250035)



CHAPTER 7

Known issues

The open and resolved bugs for a release are accessible through the Cisco Bug Search Tool.

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

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

- Known issues in Cisco UCS B-Series M5 6.0(1.260031) Server Firmware Release — None, on page 76
- Known issues in Cisco UCS B-Series M5 6.0(1.260012) Server Firmware Release — None, on page 76
- Known issues in Cisco UCS X-Series M8, M7, M6 6.0(2.260040), XE-Series M8 6.0(2.260042), C-Series M8, M7, M6 6.0(2.260044), and B-Series M6 6.0(2.260040) Server Firmware Release, on page 76
- Known issues in Cisco UCS XE-Series M8 Server Firmware Release, 6.0(1.260001) — None, on page 78
- Known issues in Cisco UCS C-Series M8 6.0(1.250194) Server Firmware Release — None, on page 78
- Known issues in Cisco UCS X-Series M8 6.0(1.252114), M7, M6 6.0(1.250179), B-Series M6, M5 6.0(1.250169), and C-Series M8, M7, M6 6.0(1.250192) Server Firmware Release — None, on page 78
- Known issues in Cisco UCS XE-Series M8 Server Firmware Release, 6.0(1.251030), on page 78
- Known issues in Cisco UCS X-Series M8, M7, M6 6.0(1.250162), B-Series M6, M5 6.0(1.250157), and C-Series M8, M7, M6 6.0(1.250174) Server Firmware Release — None, on page 79
- Known issues in Cisco UCS X-Series M8, M7, M6 6.0(1.250122), B-Series M6, M5 6.0(1.250127), and C-Series M8, M7, M6 6.0(1.250131) Server Firmware Release — None, on page 79
- Known issues in Cisco UCS C-Series M8, M7, and M6 6.0(1.250127) Server Firmware Release, on page 79

Known issues in Cisco UCS B-Series M5 6.0(1.260031) Server Firmware Release — None

Known issues in Cisco UCS B-Series M5 6.0(1.260012) Server Firmware Release — None

Known issues in Cisco UCS X-Series M8, M7, M6 6.0(2.260040), XE-Series M8 6.0(2.260042), C-Series M8, M7, M6 6.0(2.260044), and B-Series M6 6.0(2.260040) Server Firmware Release

This section provides a brief description of the known issues.

Defect ID	Description	Workaround	First Version Affected

CSCwr72707	On fully populated Cisco UCS C220 M8, C240 M8, or UCSXE130C M8 nodes with more than two Kioxia E3.S CD8P 1.9 T NVMe drives, random workload performance drops significantly during concurrent tests. Specifically, 4K random read performance may drop from a rated 1,600kIOPS per drive to approximately 680k Input/Output Operations Per Second (IOPS) per drive during concurrent operations. Single drive tests meet expected performance, indicating the issue only occurs with multi-drive setups	To resolve this performance bottleneck, apply the following Intel-recommended kernel tuning parameters in the Red Hat Enterprise Linux (RHEL) boot configuration:
		• For single-drive configurations: Add the following to the RHEL kernel command line:
		`intel_pstate=disable pcie_aspm.policy=performance pci=pcie_bus_safe`
		• For multi-drive (fully populated) configurations: Add the following to the RHEL kernel command line:
		`intel_pstate=disable pcie_aspm.policy=performance pci=pcie_bus_safe nvme.poll_queues=32 intel_iommu=on`
			X-series: 6.0(2.260040)
			XE-series: 6.0(2.260042)
			C-series: 6.0(2.260044)
			B-series: 6.0(2.260040)

Known issues in Cisco UCS XE-Series M8 Server Firmware Release, 6.0(1.260001) — None

Known issues in Cisco UCS C-Series M8 6.0(1.250194) Server Firmware Release — None

Known issues in Cisco UCS X-Series M8 6.0(1.252114), M7, M6 6.0(1.250179), B-Series M6, M5 6.0(1.250169), and C-Series M8, M7, M6 6.0(1.250192) Server Firmware Release — None

Known issues in Cisco UCS XE-Series M8 Server Firmware Release, 6.0(1.251030)

This section provides a brief description of the known issues.

Defect ID	Description	Workaround	First Version Affected
CSCws25068	When installing Ubuntu 24.04.3 with kernel version 6.8.0-71 on the Unified Edge server, the integrated network card (ICE driver) is not detected, preventing network configuration and connectivity. This issue occurs because kernel 6.8.0-71 lacks ICE driver support for the NIC on this platform.	1. Download the GA ISO from the Ubuntu Noble Release Page and install it using a bootable USB or virtual media 2. Download the required 6.8.0-80 kernel packages (`.deb` files) from the Ubuntu Security Pool. 3. Place all `.deb` files (`linux-image`, `linux-headers`, `linux-modules`, `linux-modules-extra`, `linux-tools`) in a folder and create an ISO using a tool like genisoimage or mkisofs. 4. Mount the ISO on the server after installing Ubuntu. 5. Install the kernel packages using `dpkg -i *.deb`. 6. Reboot the server and verify the kernel version is 6.8.0-80. The integrated network card will now be detected and available for configuration.	6.0(1.251030)

Known issues in Cisco UCS X-Series M8, M7, M6 6.0(1.250162), B-Series M6, M5 6.0(1.250157), and C-Series M8, M7, M6 6.0(1.250174) Server Firmware Release — None

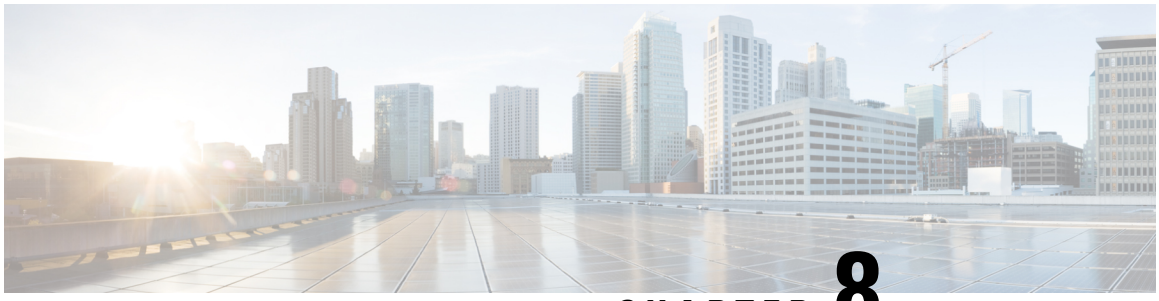
Known issues in Cisco UCS X-Series M8, M7, M6 6.0(1.250122), B-Series M6, M5 6.0(1.250127), and C-Series M8, M7, M6 6.0(1.250131) Server Firmware Release — None

Known issues in Cisco UCS C-Series M8, M7, and M6 6.0(1.250127) Server Firmware Release

This section provides a brief description of the known issues.

Defect ID	Description	Workaround	First Version Affected
CSCwn95239	On Cisco UCS C-Series servers, the server may fail to power on due to BIOS corruption. The following message is displayed: "Power on failure asserted [Power on Fail, Server failed to power-on]." This issue can occur in the following scenarios, especially when BIOS update operations are disrupted: • Interrupting a BIOS flash or update (for example, forcing a power cycle during the update). • Initiating a CMOS clear operation during a BIOS update. • Restoring factory defaults during a BIOS update. • Rebooting Cisco IMC during a BIOS update. • Performing other unexpected operations that disrupt the BIOS update process.	Do one of these: • Reboot of CIMC. In-turn, recovery mechanism will start that is bios activation. • Activate of bacup BIOS. • Update and activate BIOS.	4.3(6.250039)

Defect ID	Description	Workaround	First Version Affected
CSCwo68248	On Cisco UCS C220 M7 and C240 M7 servers running HUU 4.3(3.240xxx) level firmware with 2 PCIe VICs and 1 MLOM VIC, upgrading the server firmware to HUU 4.3(4.xxxxxx), 4.3(5.xxxxxx), 4.3(6.xxxxx), or later using the Redfish API interface may cause the UCSUpdate task to falsely report an update failure for the PCIe VIC (riser1) through which CiscoCard mode is configured. However, the firmware is actually updated and activated successfully in the background. **Note** In the mentioned HUU version numbers, "xxxx" represents all versions available within the series.	There is no workaround. Ignore the false failure update.	4.3(3.240043)



CHAPTER 8

Compatibility

• Cross-Version Firmware Support, on page 83

Cross-Version Firmware Support

Note The three-part version number format, such as 4.3(6) or 6.0(1), represents a general version series. For example, 4.3(6) indicates all firmware versions that start with 4.3(6), encompassing detailed subversions such as 4.3(6.260058) and 4.3(6.260054). Similarly, 6.0(1) indicates all firmware versions that start with 6.0(1), encompassing detailed subversions such as 6.0(1.260003) and 6.0(1.250127). For detailed information about specific firmware versions and their equivalencies across Cisco Intersight, Cisco Integrated Management Controller (Cisco IMC), and Cisco UCS Manager, see the Cisco UCS Equivalency Matrix.

XE-Series Server Firmware Version	eCMC Infrastructure Firmware Version	
	6.0(1)	6.0(2)
6.0(2)	Yes	Yes
6.0(1)	Yes	Yes

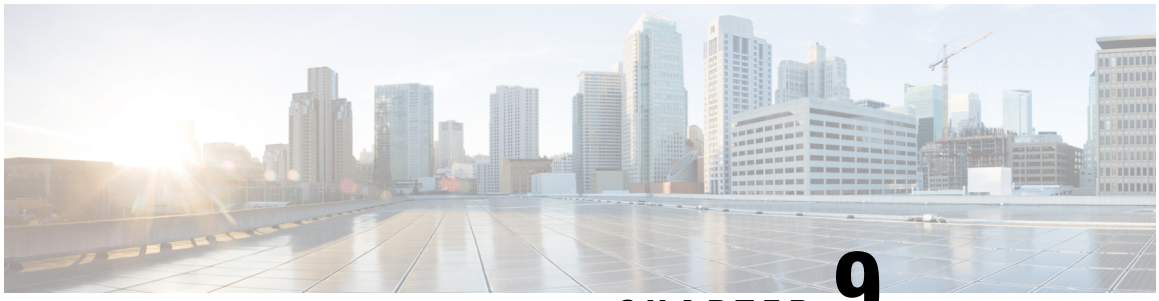
X-Series Server Firmware Version	Infrastructure Firmware Version										
	4.1(3)	4.2(1)	4.2(2)	4.2(3)	4.3(2)	4.3(3)	4.3(4)	4.3(5)	4.3(6)	6.0(1)	6.0(2)
6.0(2)	N/A	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
6.0(1)	N/A	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5.4(0)	N/A	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5.3(0)	N/A	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5.2(2)	N/A	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5.2(1)	N/A	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

5.2(0)	N/A	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5.1(1)	N/A	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5.1(0)	N/A	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5.0(4)	N/A	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5.0(2)	N/A	Yes	Yes	Yes	No	No	No	No	No	No	No
5.0(1)	N/A	Yes	Yes	Yes	No	No	No	No	No	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(4)**	**4.3(5)**	**4.3(6)**	**6.0(1)**	**6.0(2)**
6.0(2)	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
6.0(1)	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4.3(6)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4.3(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4.3(4)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4.3(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4.3(2)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4.3(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4.2(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4.2(2)	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No
4.2(1)	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No
4.1(3)	Yes	Yes	Yes	Yes	No	No	No	No	No	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)**	**4.3(4)**	**4.3(5)**	**4.3(6)**	**6.0(1)**	**6.0(2)**
6.0(2)	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
6.0(1)	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5.4(0)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5.3(0)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5.2(2)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

5.2(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5.2(0)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5.1(0)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4.3(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4.3(2)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4.2(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4.2(2)	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No
4.2(1)	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No
4.1(3)	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No



CHAPTER 9

Related resources

- Related resources, on page 87

Related resources

- Release Notes and Release Bundles for Cisco Intersight
- Cisco Baseboard Management Controller Release Notes for Cisco UCS C885A M8 Rack Server
- Release Notes for Cisco UCS Manager
- Release Notes for Cisco UCS Rack Server Software
- Cisco UCS Manager and Intersight Release Strategy
- Cisco UCS Equivalency Matrix for Cisco Intersight, Cisco IMC, and Cisco UCS Manager
- Release Notes for Cisco Intersight Unified Edge eCMC Infrastructure Firmware Release, 6.0
- Release Notes and Release Bundles for Unified Edge
- Managing Firmware in Unified Edge

Related resources

© 2025–2026 Cisco Systems, Inc. All rights reserved.