Release Notes for Cisco UCS Manager, Release 6.0

First Published: 2025-09-02

Last Modified: 2026-10-01

Cisco UCS Manager

Cisco UCS™ Manager, Release 6.0, provides unified, embedded management for all software and hardware components of the Cisco Unified Computing System™ (Cisco UCS). It supports management across multiple chassis, Cisco UCS servers, and thousands of virtual machines. Cisco UCS Manager manages Cisco UCS as a single entity using an intuitive graphical user interface (GUI), a command-line interface (CLI), or an XML API. This enables comprehensive access to all Cisco UCS Manager functions. For more details, visit Cisco UCS Manager on Cisco.com.

This document provides information about new features, resolved caveats, open caveats, and workarounds for Cisco UCS Manager, Release 6.0. It also includes:

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

Revision History

Table 1: Release 6.0(2)

Release	Date	Description
6.0(2e)	October 9, 2026	Updated Security Fixes in Release 6.0(2e), on page 8.
6.0(2e) and 6.0(2d)	October 1, 2026	Updated: • Security Fixes in Release 6.0(2e), on page 8 • Security Fixes in Release 6.0(2d), on page 9
6.0(2e)	September 23, 2026	Created release notes for Cisco UCS Manager Release 6.0(2e).
6.0(2d)	June 25, 2026	Created release notes for Cisco UCS Manager Release 6.0(2d).

Release	Date	Description
6.0(2c)	April 23, 2026	Created release notes for Cisco UCS Manager Release 6.0(2c).
6.0(2b)	March 16, 2026	Created release notes for Cisco UCS Manager Release 6.0(2b).

Table 2: Release 6.0(1)

Release	Date	Description
6.0(1h)	March 27, 2026	Created release notes for Cisco UCS Manager Release 6.0(1h).
6.0(1f)	February 06, 2026	Created release notes for Cisco UCS Manager Release 6.0(1f).
6.0(1e)	December 18, 2025	Created release notes for Cisco UCS Manager Release 6.0(1e).
6.0(1b)	December 09, 2025	Added CSCws30219 under Open Caveats in Release 6.0(1b), on page 55.
6.0(1d)	November 12, 2025	Created release notes for Cisco UCS Manager Release 6.0(1d).
6.0(1c)	October 09, 2025	Created release notes for Cisco UCS Manager Release 6.0(1c).
6.0(1b)	September 02, 2025	Created release notes for Cisco UCS Manager Release 6.0(1b).

What's New

New Hardware Features

- New Hardware in Release 6.0(2e)- None
- New Hardware in Release 6.0(2d), on page 3
- New Hardware in Release 6.0(2c), on page 3
- New Hardware in Release 6.0(2b), on page 4
- New Hardware in Release 6.0(1h)- None
- New Hardware in Release 6.0(1f)- None
- New Hardware in Release 6.0(1e), on page 4
- New Hardware in Release 6.0(1d)- None
- New Hardware in Release 6.0(1c)- None

- New Hardware in Release 6.0(1b), on page 4

New Software Features

- New Software features in Release 6.0(2e)- None
- New Software features in Release 6.0(2d)- None
- New Software features in Release 6.0(2c)- None

- New Software Feature in Release 6.0(2b), on page 5

- New Software features in Release 6.0(1h)- None
- New Software features in Release 6.0(1f)- None
- New Software features in Release 6.0(1e)- None
- New Software features in Release 6.0(1d)- None
- New Software features in Release 6.0(1c)- None

- New Software Feature in Release 6.0(1b), on page 7

New Hardware Features

New Hardware in Release 6.0(2d)

Peripherals

Following peripherals are supported from release 6.0(2d) onwards:

- NVIDIA RTX Pro 4500 GPU 160W 32GB Gen5 FHFL 1-slot (UCSX-GPU-RTXP4500) with Cisco UCS C245 M8 and C240 M8 servers.
- NVIDIA RTX Pro 6000D GPU 600W, 84GB, 2-slot FHFL PCIe GPU (UCSC-GPU-RTX6000D) with Cisco UCS C240 M8 servers.

New Hardware in Release 6.0(2c)

Peripherals

Following peripherals are supported from release 6.0(2c) onwards:

- NVIDIA OEM BlueField-3 B3220 DPU 2x200G QSFP112, Crypto Disabled (UCSC-P-N3220) with Cisco UCS C240 M7, C245 M8 and C240 M8 servers
- NVIDIA BlueField-3 B3220L SuperNIC 2x200G QSFP112, PCIe Gen5.0 x16, Crypto Disabled (UCSC-P-N3220L) with Cisco UCS C240 M7, C225 M8, C245 M8 , C220 M8 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 Release 6.0(2b)

Cisco UCS 6652 Fabric Interconnect

Cisco UCS 6652 Fabric Interconnect—The Cisco UCS 6652 Fabric Interconnect is a 1-rack unit (RU), fixed-port system designed for Top-of-Rack deployment in data centers. The fabric interconnect has both Ethernet and unified ports. Unified ports provide Fibre Channel over Ethernet (FCoE), Fibre Channel, NVMe over Fabric, and Ethernet. By supporting these different protocols, you can use a single multi-protocol Virtual Interface Card (VIC) in your servers.

The Cisco UCS 6652 Fabric Interconnect supports an array of Gigabit Ethernet (GbE), Fibre Channel (FC), and Fibre Channel over Ethernet (FCoE) ports to offer connectivity to peer data center devices. This device is also ideal for high-performance, scalable, and secure networking in modern data centers.

Cisco UCS X410c M8 Compute Node

The Cisco UCS X410c M8 Compute Node is a four-socket, mission-critical server designed for demanding enterprise applications, memory-intensive workloads, and virtualization. It supports up to four Intel® Xeon 6 Processors with up to 86 cores per CPU and up to 16 TB of DDR5-6400 memory across 64 DIMM slots. Storage options include up to nine hot-pluggable EDSFF E3.S NVMe drives via a new passthrough front-mezzanine controller, or up to six 2.5-inch SAS/SATA/NVMe drives with RAID options, plus flexible boot options with M.2 SATA or NVMe drives.

The server supports Cisco UCS Virtual Interface Cards (VICs) for unified fabric connectivity, including up to 200 Gbps per server with secure boot technology. It is also managed through Cisco Intersight SaaS platform for automation and proactive support, simplifying administration and accelerating time to resolution. The system is designed to fit into the Cisco UCS X9508 Chassis, leveraging shared power, cooling, and management resources for scalable data center operations.

Peripherals

Following peripherals are supported from release 6.0(2b) onwards:

- NVIDIA Crypto B3220 DPU (UCSC-P-NC3220) with Cisco UCS C245 and C240 M8 servers
- NVIDIA Crypto B3220L SuperNIC (UCSC-P-NC3220L) with Cisco UCS C225, C245, C220, and C240 M8 servers
- Support for NVIDIA RTX Pro 6000 (UCSC-GPU-RTXP6000) with Cisco UCS C240 M8 servers

New Hardware in Release 6.0(1e)

Support for 6x 2.5" SAS/SATA/NVMe U.2 drives (HW RAID) (UCSX-RAID-M1L6) with Cisco UCS X215c M8 Compute Node.

New Hardware in Release 6.0(1b)

- Cisco UCS 6664 Fabric Interconnect—The Cisco UCS 6664 Fabric Interconnect is a 2-rack unit (RU), fixed-port system designed for Top-of-Rack deployment in data centers. The fabric interconnect has both Ethernet and unified ports. Unified ports provide Fibre Channel over Ethernet (FCoE), Fibre Channel, NVMe over Fabric, and Ethernet. By supporting these different protocols, you can use a single multi-protocol Virtual Interface Card (VIC) in your servers.

The Cisco UCS 6664 Fabric Interconnect supports an array of Gigabit Ethernet (GbE), Fibre Channel (FC), and Fibre Channel over Ethernet (FCoE) ports to offer connectivity to peer data center devices. This device is also ideal for high-performance, scalable, and secure networking in modern data centers.

- Support for UCSX-X10C-PTE3 Pass Controller on Cisco UCS X215c M8 Compute Node.
- Support for 30TB 2.5 inch pTLC Micron 6550 NVMe drive on Cisco UCS C225 M8 servers
- Cisco UCS Manager introduces 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.

New Software Features

New Software Feature in Release 6.0(2b)

New Features

Support for the following software features:

- Enhanced Fabric Interconnect Audit Logs to provide granular monitoring and tracking of user and system activities on Cisco UCS 6600, 6500, and 6400 Series Fabric Interconnects using the Linux Audit Framework (auditd). You can enable or disable this service, configure the logging severity, and also selectively monitor various rules for enhanced security and compliance.
- Cisco UCS Manager now supports integrated firmware upgrades for 64-Gigabit Fibre Channel (FC) Small Form-Factor Pluggable (SFP) transceivers on Cisco UCS 6600 Series Fabric Interconnects. This feature allows you to resolve operational issues by updating transceiver firmware, ensuring optimal link stability and fabric compatibility. Proactive system faults notify you when an upgrade is required, streamlining maintenance workflows and ensuring the health of critical networking components.
- Added support for Secure Hash Algorithm 512 (SHA 512) authentication in SNMP configuration, enabling stronger, high-assurance security for SNMP communications.
- Cisco UCS Manager enhances security management by introducing advanced encryption management capabilities with primary keys. These capabilities provide comprehensive data protection and enable secure management operations across the UCS environment.
- Fabric Interconnect now enforces complex password requirements by default. Administrator users must adhere to these security standards when creating new user accounts or updating existing credentials.
- Enhanced Security Configuration and Alert Management in Cisco UCS Manager. Cisco UCS Manager now enforces Secure Boot by default to strengthen platform integrity. For environments that require additional time to transition to updated security standards, there is the option to suppress warning faults.
- Cisco UCS 6600 Series Fabric Interconnects (UCS-FI-6652 and UCS-FI-6664) now support 50 Gbps speed on unified Ethernet ports, delivering greater bandwidth and enhanced connectivity, which enables more efficient network performance and scalability.
- Migration support for Cisco UCS 6600 Series Fabric Interconnect, including:
  - UCS-FI-6454 to UCS-FI-6652
  - UCS-FI-64108 to UCS-FI-6652
  - UCS-FI-6536 to UCS-FI-6652

- Cisco UCS Manager introduces unified infrastructure firmware management for Cisco UCS 6600 Series and 6500 Series Fabric Interconnects and deprecates support for Service Pack firmware packages; separate Service Pack files and its Startup Version are no longer utilized. All maintenance fixes, security patches, and updates are now delivered within a single, unified Infrastructure Software Bundle. Lightweight upgrades are not supported in this unified model, requiring all infrastructure upgrades to follow the standard Auto Install process. The standard Auto Install process requires necessary reboots of the Fabric Interconnects to ensure all consolidated fixes are correctly applied.
- Added support for configuration of MTU values up to 9158 bytes per vNIC in Cisco UCS Manager. This enhancement enables jumbo frame support for advanced networking and storage use cases on Cisco UCS 15000 VIC adapters.
- Cisco UCS Manager now supports up to 16,384 LUNs per vHBA (FC-Initiator) for supported Cisco UCS VIC adapters. This enables better compatibility with modern storage arrays and host OSes supporting large LUN counts.
- Support for NFS over RDMA is available with Cisco UCS VIC 15000 Series adapters on Linux.
- Cisco UCS Manager now supports displaying real-time traffic rates in Gbps and packets per second (pps) for Virtual Ethernet (veth) and Virtual Fibre Channel (vfc) interfaces via the CLI. This enhancement allows for more effective troubleshooting of network performance and congestion.
- Cisco UCS Manager now supports IPv6 protocols for Key Management Interoperability Protocol (KMIP) server integration. This enhancement enables compliance with regulatory and industry standards requiring IPv6 support in UCS Manager.
- Added a new configuration option for **Spanning Tree Protocol (STP) Faults** that allows admin user to enable or disable the raising of STP-related faults. When disabled, existing faults are cleared and new faults are suppressed; when enabled, Cisco UCS Manager begins raising new faults. This enhancement provides administrators with precise control over STP fault monitoring, improving network management and operational stability.

Unified Infrastructure Bundle for Release 6.0(2b)

The 6.0(2b) release introduces a **unified infrastructure bundle** that consolidates the infrastructure firmware for the Cisco UCS 6600, 6500, 6400 series FIs, and Cisco UCSX-S9108-100G into a single package. This unified bundle simplifies management by replacing multiple individual infrastructure bundles with a single consolidated bundle.

This change applies exclusively to the infrastructure bundle. The B-Series and C-Series server bundles remain unchanged and continue to be delivered as separate bundles.

Although the unified infrastructure bundle is available starting with the 6.0(2b) release, it **cannot be used for upgrades in this release**. You must continue to use the individual platform infrastructure bundles for upgrades.

Both the unified bundle and the individual platform bundles are available in this release to support your current upgrade paths. In future releases, the unified bundle is designed to be used for upgrade purposes once it becomes supported.

- Introduction of a unified infrastructure bundle for Cisco UCS 6600, 6500, 6400 series FIs, and Cisco UCSX-S9108-100G.
- Server bundles (B-Series and C-Series) remain unchanged
- Unified bundle is available from 6.0(2b) but not supported for upgrades in this release

- Continue using individual bundles for upgrades to 6.0(2b) release
- Both unified and individual bundles are provided in this release
- The unified bundle is intended to simplify upgrade management in future releases

New Software Feature in Release 6.0(1b)

Support for the following software features:

- Fabric Interconnect Audit Log support using the Linux Audit Framework (auditd), providing comprehensive monitoring and tracking of user and system activities on Cisco UCS 6600, 6500, and 6400 Series Fabric Interconnects. This feature enables enhanced security and compliance by recording activities into Fabric Interconnect Audit Log files.
- Cisco UCS X-Series Direct (Fabric Interconnect 9108 100G) now supports Cisco UCS C-Series rack servers, enabling unified management of both UCS X-Series compute nodes and C-Series servers in one domain. It also adds secondary chassis support, allowing deployment of a second UCS X9508 chassis and up to 20 servers in a single X-Direct domain. These enhancements improve scalability and simplify data center hardware management.
- iSCSI boot support using Internet Protocol version 6 (IPv6) for Cisco UCS servers, enabling seamless integration into IPv6-capable IP networks. This addresses IPv4 limitations and offers improved scalability and management for next-generation infrastructure deployments.
- Support for AES master key and MACsec (Type-6 [AES], Type-0, and Type-7 encryption) for Ethernet uplink ports is now available on Cisco UCS 6664 Fabric Interconnects and Cisco UCS X-Series Direct (Cisco UCS Fabric Interconnects 9108 100G).
- Support for ERSPAN on Cisco UCS X-Series Direct (Cisco UCS Fabric Interconnects 9108 100G).
- Migration support for Cisco UCS 6600 Series Fabric Interconnect, including:
  - UCS-FI-6454 to UCS-FI-6664
  - UCS-FI-64108 to UCS-FI-6664
  - UCS-FI-6536 to UCS-FI-6664
- Added warning message for Native VLAN Configuration changes on vNICs, highlighting the requirement for a port flap and a brief connectivity impact (approximately 20–40 seconds) when the Native VLAN is modified. This enhancement helps administrators better plan for and manage VLAN changes.
- Support for KVM direct access over inband on Cisco UCS C-Series M8, M7, and M6 servers, enabling administrators to securely access and manage server consoles directly over the inband network and improving operational efficiency and flexibility for Cisco UCS C-Series servers.
- Support for secure deletion of all data on Cisco UCS 6400, 6500, 6600 Series, and X-Series Direct Fabric Interconnect using the Command Line Interface (CLI). This enhancement ensures customer data privacy by permanently deleting all data, eliminating the possibility of data retrieval or recovery.
- Enhanced Login Profile security with configurable rules for user login attempts, enabling administrators to monitor and audit access. The system can block further logins for a set time after a specified number of failed attempts to prevent unauthorized access. Additionally, Cisco UCS Manager now generates syslog messages for authentication failures, including details such as user ID, domain ID, IP address, and account status.

Security Fixes

Security Fixes in Release 6.0(2e)

Security Hardening Updates

Cisco NX-OS Software updates include security hardening to address multiple vulnerabilities identified during internal testing. Cisco is not aware of these vulnerabilities being actively exploited. Related issues are grouped by Common Weakness Enumeration (CWE) and associated with a single Common Vulnerabilities and Exposures (CVE) identifier to support customer remediation and disclosure.

Cisco has released software updates that address these vulnerabilities. There are no workarounds that address these vulnerabilities.

- CVE-2026-76453
- CVE-2026-76455
- CVE-2026-76456
- CVE-2026-76457
- CVE-2026-76458
- CVE-2026-76459

This advisory is available at the following link:

Cisco NX-OS Software Security Hardening Release: October 2026

Defect ID - CSCwt77804

A vulnerability in the Unified Extensible Firmware Interface (UEFI) Shell implementation of all Cisco UCS B-series and C-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.

- CVE-2026-20293

This advisory is available at the following link:

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

Security Fixes in Release 6.0(2d)

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 Release 6.0(2c)

There are no new security fixes in release 6.0(2c).

Security Fixes in Release 6.0(2b)

Defect ID - CSCwr50426

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

- 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-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

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

- 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

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

- CVE-2021-0920—A race condition in the Unix domain socket implementation (unix_scm_to_skb in af_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

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

- 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

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

- 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 (CRLF injection) 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-2024-38428—Wget before 1.24.5 is vulnerable to a flaw where it fails to properly parse userinfo 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

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

- 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 readdir_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-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 hostname.
- 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-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 large UDP 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 2.27 leads 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-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-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-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—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-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

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

- 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-8 characters.
- 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-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-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-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

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

- 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

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

- CVE-2023-38545—A high-severity heap-based buffer overflow vulnerability in curl's SOCKS5 proxy handshake occurs when a hostname 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

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

- 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-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

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

- 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-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 win32/perlhost.h in 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-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 Release 6.0(1h)

There are no new security fixes in release 6.0(1h).

Security Fixes in Release 6.0(1f)

There are no new security fixes in release 6.0(1f).

Security Fixes in Release 6.0(1e)

There are no new security fixes in release 6.0(1e).

Security Fixes in Release 6.0(1d)

Defect ID - CSCwq36167

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

- CVE-2025-20067—Observable timing discrepancy in firmware for some Intel® CSME and Intel® 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 products UCS C-Series M7 Rack Servers and UCS X-Series M7 Compute Nodes 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® TDX may allow a privileged user to potentially enable escalation of privilege via local access.
- CVE-2025-20053—Improper buffer restrictions for some Intel® Xeon® 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® Xeon® 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® 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® Xeon® 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® 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 Release 6.0(1c)

There are no new security fixes in release 6.0(1c).

Security Fixes in Release 6.0(1b)

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.

Defect ID - CSCwb83414

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

- CVE-2009-5155—The glob implementation in the GNU C Library (glibc) does not properly handle long patterns, which may allow context-dependent attackers to cause a denial of service or possibly execute arbitrary code via a crafted pattern.
- CVE-2010-3192—The GNU C Library (glibc) does not properly restrict the use of the LD_AUDIT environment variable for setuid/setgid binaries, which allows local users to gain privileges by executing setuid programs with this variable set.
- CVE-2013-0242—The iconv program in GNU C Library (glibc) does not properly handle certain invalid multi-byte input sequences, which could allow remote attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2014-4043—The wordexp function in GNU C Library (glibc) allows context-dependent attackers to bypass intended restrictions via shell metacharacters, which are not properly handled in certain cases.
- CVE-2014-9402—The __hcreate_r function in GNU C Library (glibc) does not properly check for integer overflows, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2014-9761—The gethostbyname function in GNU C Library (glibc) does not properly handle long hostnames, which allows remote attackers to cause a denial of service or possibly have unspecified other impact.
- CVE-2015-5180—The iconv function in GNU C Library (glibc) does not properly handle certain input sequences, which allows attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2015-8776—The catopen function in GNU C Library (glibc) does not properly handle negative values, which could allow local users to cause a denial of service or possibly execute arbitrary code.

- CVE-2015-8777—The regcomp function in GNU C Library (glibc) may allow context-dependent attackers to cause a denial of service or possibly execute arbitrary code via a crafted regular expression.
- CVE-2015-8778—The getnetbyname function in GNU C Library (glibc) does not properly handle long network names, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2015-8779—The getaliasbyname function in GNU C Library (glibc) does not properly handle long alias names, which could allow attackers to cause a denial of service or potentially execute arbitrary code.
- CVE-2015-8982—The nan, nanf, and nanl functions in GNU C Library (glibc) do not properly handle certain malformed strings, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2015-8983—The strftime function in GNU C Library (glibc) does not properly handle certain format strings, which could allow attackers to cause a denial of service or potentially execute arbitrary code.
- CVE-2015-8984—The fnmatch function in GNU C Library (glibc) does not properly handle certain patterns, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2015-8985—The glob function in GNU C Library (glibc) does not properly handle certain patterns, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2016-10228—The iconv program in GNU C Library (glibc) does not properly handle certain malformed input sequences, which could allow attackers to cause a denial of service or potentially execute arbitrary code.
- CVE-2016-10739—The getaddrinfo function in GNU C Library (glibc) does not properly handle large AF_INET6 responses, which could allow remote attackers to cause a denial of service or potentially execute arbitrary code.
- CVE-2016-1234—The send_dg function in the resolver in GNU C Library (glibc) does not properly handle certain responses, which could allow remote attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2016-4429—The resolver in GNU C Library (glibc) does not properly handle crafted DNS responses, which could allow remote attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2017-1000366—The dynamic linker in GNU C Library (glibc) does not properly handle certain environment variables, which could allow local attackers to gain privileges or bypass security restrictions.
- CVE-2017-12132—The _dl_init_paths function in GNU C Library (glibc) does not properly process certain environment variables, which could allow local users to gain elevated privileges or bypass security restrictions.
- CVE-2017-15670—The glob function in GNU C Library (glibc) does not properly handle certain patterns, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2017-15671—The glob function in GNU C Library (glibc) does not properly handle memory allocation failures, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2017-15804—The glob function in GNU C Library (glibc) does not properly handle certain file system conditions, which could allow attackers to cause a denial of service or possibly execute arbitrary code.

- CVE-2018-1000001—The realpath function in GNU C Library (glibc) does not properly handle long paths, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2018-11236—The GNU C Library (glibc) does not properly restrict stack pointer usage in certain conditions, which could allow local attackers to execute arbitrary code or cause a denial of service.
- CVE-2018-11237—The GNU C Library (glibc) may allow attackers to cause a denial of service or possibly execute arbitrary code via crafted input that triggers incorrect handling of certain memory operations.
- CVE-2018-19591—The getcwd function in GNU C Library (glibc) does not properly handle very long directory names, which could allow local attackers to cause a denial of service or potentially execute arbitrary code.
- CVE-2018-20796—The glob function in GNU C Library (glibc) does not properly handle crafted patterns, which could allow attackers to cause a denial of service or potentially execute arbitrary code.
- CVE-2018-6485—The _dl_map_object_from_fd function in GNU C Library (glibc) does not properly handle certain ELF files, which could allow local attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2019-25013—The iconv function in GNU C Library (glibc) does not properly handle certain input sequences, which could allow attackers to cause a denial of service or potentially execute arbitrary code.
- CVE-2019-6488—The glob function in GNU C Library (glibc) does not properly handle memory allocation failures, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2019-7309—The glob function in GNU C Library (glibc) does not properly handle crafted patterns in certain conditions, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2019-9169—The __libc_open function in GNU C Library (glibc) does not properly handle file descriptors in certain situations, which could allow local attackers to cause a denial of service or potentially execute arbitrary code.
- CVE-2020-10029—The memmem function in GNU C Library (glibc) on 32-bit systems may read out of bounds, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2020-1751—The nss_dns module in GNU C Library (glibc) does not properly handle crafted DNS responses, which could allow remote attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2020-1752—The getaddrinfo function in GNU C Library (glibc) does not properly handle certain crafted responses, which could allow remote attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2020-27618—The iconv function in GNU C Library (glibc) does not properly handle certain input sequences, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2020-29573—The qsort function in GNU C Library (glibc) does not properly check for pointer overflows, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2020-6096—The x86-64 memcpy function in GNU C Library (glibc) does not properly handle overlapping memory regions, which could allow attackers to cause a denial of service or possibly execute arbitrary code.

- CVE-2021-3326—The mq_notify function in GNU C Library (glibc) does not properly handle certain parameters, which could allow local attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2021-35942—The wordexp function in GNU C Library (glibc) does not properly handle crafted patterns, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2021-38604—The iconv function in GNU C Library (glibc) does not properly handle certain input sequences, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2022-23218—The iconv function in GNU C Library (glibc) does not properly handle certain malformed input sequences, which could allow attackers to cause a denial of service or potentially execute arbitrary code.
- CVE-2022-23219—The iconv function in GNU C Library (glibc) does not properly handle certain malformed input sequences, which could allow attackers to cause a denial of service or potentially execute arbitrary 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 - CSCwb84351

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

- CVE-2015-5602—sudo before 1.8.14 does not properly parse sudoers rules, which could allow local users to bypass intended restrictions and execute arbitrary commands via a user specification containing a netgroup that is followed by an exclusion (exclamation mark) operator.
- CVE-2016-7076—sudo before 1.8.18 does not properly manage the TZ environment variable, allowing local users to bypass security restrictions or possibly execute arbitrary code via a specially crafted value of TZ in the environment of a sudo command.
- CVE-2017-1000367—In Sudo before 1.8.20, an attacker with sudo privileges may be able to run arbitrary commands as root due to an unsafe library search path, potentially resulting in privilege escalation.
- CVE-2017-1000368—Sudo before 1.8.20 improperly handles certain command line arguments, allowing local users to obtain unintended access or execute arbitrary commands as another user by leveraging a race condition.
- CVE-2019-14287—A flaw in Sudo before 1.8.28 allows a user with permission to run commands as any user except root to execute commands as root by specifying the user ID -1 or 4294967295.
- CVE-2019-18634—Sudo before 1.8.26 does not properly handle the pwfeedback option, which can allow a local user to cause a stack-based buffer overflow and potentially execute arbitrary code or escalate privileges.
- CVE-2021-23239—Sudo before 1.9.5p2 incorrectly handles certain sudoers rules for Runas user specifications, which could allow users to bypass security policies and execute commands as unintended users.
- CVE-2021-23240—Sudo before 1.9.5p2 may allow a local user to bypass Runas user restrictions due to incorrect parsing of sudoers files, enabling the execution of commands as a user other than the one intended by policy.

- CVE-2021-3156—A heap-based buffer overflow vulnerability in Sudo before 1.9.5p2, known as "Baron Samedit," allows local users to gain root privileges by triggering improper handling of command line arguments.

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 - CSCwf97363

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

- CVE-2012-0876—OpenSSL before 1.0.0h and 1.0.1-beta before 1.0.1-beta3 allows remote attackers to cause a denial of service via a crafted record that triggers an out-of-bounds read.
- CVE-2012-2135—Python before 2.7.3 and 3.x before 3.2.3 does not properly handle Unicode strings in the urllib module, which could allow remote attackers to conduct cross-site scripting (XSS) attacks or obtain sensitive information.
- CVE-2013-1753—Python before 2.7.5 and 3.x before 3.3.2 allows remote attackers to cause a denial of service via crafted input to the SSL module, resulting in excessive CPU consumption.
- CVE-2013-2099—Multiple integer overflow vulnerabilities in Python, including in the buffer and unicodeobject modules, could allow remote attackers to execute arbitrary code or cause a denial of service.
- CVE-2013-4238—OpenSSL before 1.0.1e does not properly handle certain DTLS retransmissions, which allows remote attackers to cause a denial of service via crafted DTLS packets.
- CVE-2013-7040—Python 2.7 before 2.7.7 and 3.x before 3.3.3 does not properly handle certain SSL certificate attributes, which could allow remote attackers to spoof SSL servers via crafted certificates.
- CVE-2013-7338—Python 2.7 before 2.7.7 and 3.x before 3.3.3 allows remote attackers to cause a denial of service via crafted input that triggers an infinite loop in the SSL module.
- CVE-2013-7440—The Python CGIHTTPServer module before 2.7.9 and 3.x before 3.4.3 allows remote attackers to execute arbitrary code via crafted HTTP requests that inject shell commands.
- CVE-2014-0224—OpenSSL before 1.0.1h allows man-in-the-middle attackers to decrypt and modify traffic via a flaw in the SSL/TLS handshake process when both client and server are vulnerable.
- CVE-2014-1912—Python 2.7 before 2.7.7 and 3.x before 3.3.3 allows remote attackers to cause a denial of service via crafted input to the socket module, which can trigger memory corruption.
- CVE-2014-2667—The urllib3 library before version 1.8 does not properly handle subjectAltName fields in X.509 certificates, which could allow remote attackers to spoof SSL servers via crafted certificates.
- CVE-2014-4616—OpenSSL before 1.0.1i does not properly restrict processing of DTLS packets, which allows remote attackers to cause a denial of service via crafted DTLS handshake messages.
- CVE-2014-4650—The ssl module in Python before 2.7.8 and 3.x before 3.4.2 does not properly handle certain TLS handshake messages, which could allow remote attackers to cause a denial of service.
- CVE-2014-7185—Python before 2.7.9 and 3.x before 3.4.3 allows remote attackers to execute arbitrary code via crafted pickle data that triggers unsafe loading.
- CVE-2014-9365—The Python email module before 2.7.9 and 3.x before 3.4.3 does not properly handle certain headers, which could allow remote attackers to conduct header injection attacks.

- CVE-2015-1283—Integer overflow in the zipimport module in Python before 2.7.9 and 3.x before 3.4.3 could allow attackers to execute arbitrary code or cause a denial of service via a crafted ZIP archive.
- CVE-2015-20107—Python 3.10.0 through 3.10.6 and 3.11.0a1 through 3.11.0b3 allows command injection via the mailcap module when parsing certain files, potentially allowing attackers to execute arbitrary commands.
- CVE-2015-5652—OpenSSL before 1.0.2d and 1.0.1p does not properly validate certain ASN.1 structures, which could allow remote attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2016-0718—The _json module in Python before 2.7.11 and 3.x before 3.4.4 allows context-dependent attackers to cause a denial of service via a crafted JSON document that triggers an incorrect exception.
- CVE-2016-0772—The ssl.match_hostname function in Python before 2.7.10 and 3.x before 3.4.4 does not properly match IP addresses in hostnames, which could allow attackers to spoof SSL servers.
- CVE-2016-1000110—The urllib3 and requests libraries, before urllib3 1.23 and requests 2.20.0, do not properly handle certain HTTP headers, which could allow remote attackers to conduct CRLF injection attacks via crafted headers.
- CVE-2016-2183—The SWEET32 attack affects 64-bit block ciphers in TLS, such as 3DES and Blowfish, allowing remote attackers to recover plaintext data via a birthday attack against long-duration encrypted sessions.
- CVE-2016-3189—Python before 2.7.12 and 3.x before 3.5.2 does not properly validate certificates when using the ssl.match_hostname function, which could allow remote attackers to spoof SSL servers.
- CVE-2016-4472—Python before 2.7.13 and 3.x before 3.5.2 does not properly handle certain HTTP responses in the httplib module, which could allow remote attackers to conduct HTTP header injection attacks.
- CVE-2016-5636—OpenSSL before 1.0.2i and 1.0.1u does not properly validate certain certificate fields, which could allow remote attackers to conduct impersonation attacks or cause a denial of service.
- CVE-2016-5699—Python before 2.7.13 and 3.x before 3.5.2 does not properly handle certain HTTP responses in urllib, which could allow attackers to conduct HTTP response splitting attacks.
- CVE-2016-9063—The DES and Triple DES ciphers, as used in OpenSSL and NSS, have a birthday bound of approximately four billion blocks, allowing remote attackers to recover plaintext data via a birthday attack (SWEET32).
- CVE-2017-1000158—Python 2.7 before 2.7.13 and 3.x before 3.6.1 does not properly handle certain Unicode strings in the urllib and http libraries, which could allow remote attackers to conduct CRLF injection attacks.
- CVE-2017-9233—The _strxfrm function in Python before 2.7.14 and 3.x before 3.6.2 does not properly validate certain input, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2018-1000030—Python before 2.7.14 and 3.x before 3.6.4, when using shutil.rmtree with symlinks, may allow local attackers to delete arbitrary files via a race condition.
- CVE-2018-1000802—Python 2.7, 3.4, 3.5, and 3.6 allow local users to execute arbitrary code as root via a Trojan horse module in a local directory, which is searched before system directories when running scripts with elevated privileges.

- CVE-2018-1060—Python 2.7 before 2.7.15 and 3.x before 3.4.6 and 3.5.x before 3.5.3 does not properly handle certain regular expressions in the difflib and poplib modules, which could allow attackers to cause a denial of service.
- CVE-2018-1061—Python 2.7 before 2.7.15 and 3.x before 3.4.6 and 3.5.x before 3.5.3 allows remote attackers to cause a denial of service via a crafted email address to the email.utils.parseaddr function.
- CVE-2018-14647—The PyYAML library in versions before 4.1 allows remote attackers to execute arbitrary code via crafted YAML input, due to unsafe use of the yaml.load function.
- CVE-2018-20406—Python 2.7 before 2.7.16 and 3.x before 3.4.10, 3.5.x before 3.5.7, and 3.6.x before 3.6.9 does not properly handle certain regular expressions in the difflib module, which may allow attackers to cause a denial of service.
- CVE-2018-20852—Python 3.7.x before 3.7.4 and 3.8.x before 3.8.1 does not properly handle certain inputs in the urllib.parse module, which could allow attackers to bypass URL parsing restrictions.
- CVE-2018-25032—zlib through 1.2.11 has a memory corruption issue related to the inflateMark function, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2019-10160—Python 2.7 before 2.7.16 and 3.x before 3.7.3 does not properly handle certain regular expressions in the difflib module, which could allow attackers to cause a denial of service.
- CVE-2019-12900—zlib through 1.2.11 has a memory corruption issue in the inflate function, which could allow remote attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2019-15903—Python 2.7 before 2.7.17 and 3.x before 3.7.5 does not properly validate input in the tarfile module, which could allow remote attackers to write files outside of the intended directory via a crafted TAR archive.
- CVE-2019-16056—Python 2.7 before 2.7.17 and 3.x before 3.7.5 does not properly handle certain inputs in the http.client module, which could allow attackers to conduct HTTP header injection attacks.
- CVE-2019-16935—Python 2.7 before 2.7.18 and 3.x before 3.7.6 has an issue in the XML parsing modules (xmlrpc), which could allow remote attackers to cause a denial of service via crafted XML data.
- CVE-2019-18348—The urllib3 library before 1.25.3 does not properly remove the authorization header when a redirect to a different host occurs, which could allow remote attackers to obtain sensitive information by intercepting redirected requests.
- CVE-2019-20907—Python 3.4.x through 3.8.x mishandles certain regular expressions in the re module, which could allow attackers to cause a denial of service via a crafted regex pattern.
- CVE-2019-5010—Python before 2.7.16 and 3.x before 3.7.2 mishandles null bytes in certain inputs to the xmlrpc.client and xmlrpc.server modules, which could allow remote attackers to cause a denial of service.
- CVE-2019-9636—Python 3.x before 3.7.3 does not properly sanitize input in the urlsplit and urlparse functions, which could allow attackers to bypass security restrictions or conduct attacks such as URL spoofing.
- CVE-2019-9674—Python 3.0 through 3.7.2 mishandles certain crafted ZIP archives in the zipfile module, which could allow attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2019-9947—Python 2.7 before 2.7.16 and 3.x before 3.7.3 mishandle certain newline characters in the urllib module, which could allow attackers to conduct HTTP header injection attacks.

- CVE-2019-9948—Python 2.7 before 2.7.16 and 3.x before 3.7.3 mishandle certain inputs in the urllib module, which could allow attackers to conduct HTTP header injection attacks.
- CVE-2020-10735—Python 3.7 through 3.10 mishandles int to string conversions for large integers, which could allow attackers to cause a denial of service via excessive CPU usage.
- CVE-2020-14422—Python 2.7 before 2.7.18 and 3.x before 3.7.7 mishandles certain inputs in the http.client module, which could allow attackers to conduct HTTP header injection attacks.
- CVE-2020-15523—Python 2.7 before 2.7.18 and 3.x before 3.8.4 mishandles certain regular expressions in the difflib and poplib modules, which could allow attackers to cause a denial of service.
- CVE-2020-15801—Python 3.8.x before 3.8.5 mishandles certain inputs in the tarfile module, which could allow remote attackers to write files outside of the intended directory via a crafted TAR archive.
- CVE-2020-26116—Python 3.x before 3.9.0 mishandles certain regular expressions in the difflib module, which could allow attackers to cause a denial of service via excessive CPU consumption.
- CVE-2020-27619—Python 3.8.x before 3.8.6 mishandles certain inputs in the http.client module, which could allow attackers to conduct HTTP header injection attacks.
- CVE-2020-8315—Python 2.7 before 2.7.18 and 3.x before 3.8.3 mishandles certain inputs in the urllib module, which could allow attackers to conduct HTTP header injection attacks.
- CVE-2020-8492—Python 2.7 before 2.7.18 and 3.x before 3.8.2 mishandles certain inputs in the urllib.parse module, which could allow attackers to bypass security restrictions or conduct attacks such as URL spoofing.
- CVE-2021-23336—Python 3.6.x through 3.8.x mishandles certain URLs in the urllib.parse module, which could allow attackers to bypass security restrictions or conduct attacks such as URL spoofing.
- CVE-2021-3177—Python 3.x before 3.9.2 has a buffer overflow in the PyCArg_repr function in the ctypes module, which could allow attackers to execute arbitrary code or cause a denial of service.
- CVE-2021-3426—Python 3.7.x before 3.7.10, 3.8.x before 3.8.8, and 3.9.x before 3.9.2 mishandle certain regular expressions in the re module, which could allow attackers to cause a denial of service via excessive CPU usage.
- CVE-2021-3733—Python 3.6.x through 3.9.x mishandles certain inputs in the urllib.parse module, which could allow attackers to bypass security restrictions or conduct attacks such as URL spoofing.
- CVE-2021-3737—Python 3.6.x through 3.9.x mishandles certain inputs in the urllib.parse module, which could allow attackers to bypass security restrictions or conduct attacks such as URL spoofing.
- CVE-2021-4189—Python 3.6.x through 3.9.x mishandles certain inputs in the urllib.request module, which could allow attackers to bypass security restrictions or conduct attacks such as URL spoofing.
- CVE-2022-0391—Python 3.7.x through 3.9.x mishandles certain inputs in the urllib.parse module, which could allow attackers to bypass security restrictions or conduct attacks such as URL spoofing.
- CVE-2022-26488—Python 2.7 before 2.7.18 and 3.x before 3.8.10 mishandles certain inputs in the http.client module, which could allow attackers to conduct HTTP header injection attacks.
- CVE-2022-37454—The Python 'random' module, as used in PyCryptodome before 3.15, may generate predictable random numbers under certain conditions, which could weaken cryptographic operations and allow attackers to guess secret values.

- CVE-2022-45061—Python 3.9.x before 3.9.16, 3.10.x before 3.10.9, and 3.11.x before 3.11.1 mishandle certain regular expressions in the urllib module, which could allow attackers to cause a denial of service via excessive CPU usage.
- CVE-2023-24329—The urllib.parse module in Python 3.x before 3.10.10 and 3.11.x before 3.11.2 does not properly parse URLs containing whitespace characters, which could allow attackers to bypass security checks or conduct spoofing attacks.
- CVE-2023-27043—Python 3.7.x through 3.11.x mishandles certain inputs in the urllib.parse module, which could allow attackers to conduct HTTP header injection or other attacks by bypassing input validation.

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 - CSCwf97368

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

- CVE-2011-2939—Perl before 5.14.2 and 5.12.4 allows context-dependent attackers to execute arbitrary code or cause a denial of service via a crafted regular expression that triggers a heap-based buffer overflow.
- CVE-2012-5195—The Perl CGI module before 3.63 allows remote attackers to inject HTTP headers via newline characters in the values of certain CGI parameters.
- CVE-2012-6329—The Encode module in Perl before 5.16.1 does not properly handle certain UTF-8 input, which could allow context-dependent attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2013-1667—The CGI module in Perl before 5.14.3 and 5.16.x before 5.16.3 does not properly handle special characters in MIME headers, which could allow remote attackers to inject arbitrary HTTP headers.
- CVE-2014-4330—Perl before 5.20.1 mishandles certain crafted regular expressions, which could allow context-dependent attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2015-8853—The File::Temp module in Perl before 2.26 does not properly check permissions for temporary files, which could allow local users to obtain sensitive information or modify data via a symlink attack.
- CVE-2016-1238—Perl before 5.24.1 does not properly search for library paths, which could allow local users to execute arbitrary code via a Trojan horse module in an insecure directory.
- CVE-2016-2381—The DB_File module in Perl before 5.24.0 allows context-dependent attackers to execute arbitrary code or cause a denial of service via crafted input that triggers memory corruption.
- CVE-2017-12814—The XSLoader module in Perl before 5.24.3 and 5.26.x before 5.26.1 does not properly handle certain input, which could allow attackers to execute arbitrary code or cause a denial of service.
- CVE-2017-12837—Perl before 5.26.2 mishandles certain crafted regular expressions, which could allow context-dependent attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2017-12883—Perl before 5.26.2 mishandles certain crafted regular expressions, which could allow context-dependent attackers to cause a denial of service or possibly execute arbitrary code.

- CVE-2018-12015—The Archive::Tar module in Perl before 2.24 allows remote attackers to overwrite arbitrary files via a symlink attack in a TAR archive.
- CVE-2018-18311—Perl before 5.28.1 mishandles certain crafted regular expressions, which could allow context-dependent attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2018-18312—Perl before 5.28.1 mishandles certain crafted regular expressions, which could allow context-dependent attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2018-18313—Perl before 5.28.1 mishandles certain crafted regular expressions, which could allow context-dependent attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2018-18314—Perl before 5.28.1 mishandles certain crafted regular expressions, which could allow context-dependent attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2018-6913—The Encode module in Perl before 5.26.2 allows context-dependent attackers to cause a denial of service via crafted input that triggers a buffer overflow.
- CVE-2020-10543—Perl before 5.30.3 mishandles certain crafted regular expressions, which could allow context-dependent attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2020-10878—Perl before 5.30.3 mishandles certain crafted regular expressions, which could allow context-dependent attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2020-12723—Perl before 5.30.3 mishandles certain crafted regular expressions, which could allow context-dependent attackers to cause a denial of service or possibly execute arbitrary code.
- CVE-2023-31486—The Archive::Tar module in Perl before 2.40 does not properly validate file paths in TAR archives, which could allow attackers to write files outside of the intended directory via a crafted archive.

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 - CSCwb84668

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

- CVE-2014-9471—The chfn and chsh utilities in util-linux before 2.26 do not properly check for newline characters in user input, which could allow local users to bypass security restrictions or inject malicious content into configuration files.
- CVE-2015-4042—The su utility in util-linux before 2.26.2 does not properly clear environment variables, which could allow local users to gain privileges or bypass security restrictions via a crafted environment.
- CVE-2016-2781—The chroot utility in GNU coreutils before 8.25 does not properly drop supplementary groups before executing commands, which could allow local users to bypass intended security restrictions.
- CVE-2017-18018—runuser in util-linux before 2.30.2 does not properly clear environment variables, which could allow local users to gain privileges or bypass security restrictions via a crafted environment.

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.

Resolved Caveats

Resolved Caveats in Release 6.0(2e)

Defect ID	Symptoms	First Bundle Affected	Resolved in Release
CSCwt88208	FCPU hang on Cisco UCS VIC 1300 Series adapters is not detected, and the condition cannot be reported through a Cisco UCS Manager fault. The affected blade must be rebooted to recover. This issue is resolved.	4.3(4e)B	6.0(2e)B
CSCww40564	When connecting to an adapter through the Cisco UCS Manager or Cisco Integrated Management Controller CLI, the connection fails because the required rlogin executable is unavailable. This issue is resolved.	6.0(2b)A	6.0(2e)A
CSCwv10305	A Cisco UCS 9108 100G Fabric Interconnect can reset because of a kernel panic. This issue is resolved.	6.0(2b)A	6.0(2e)A

Resolved Caveats in Release 6.0(2d)

The following caveat is resolved in release 6.0(2d):

Defect ID	Symptoms	First Bundle 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. T 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.	4.2(3m)	6.0(2d)

Defect ID	Symptoms	First Bundle Affected	Resolved in Release
CSCwt79531	After an infrastructure upgrade on Cisco UCS systems with 6454 fabric interconnects, server discovery can fail at 25% because the svc_sam_dme process enters an incorrect state. NIC AG logs can show a memory allocation failure when this issue occurs. This issue is resolved.	4.3(4e)A	6.0(2d)
CSCwt96184	After server decommission and recommission for the Cisco UCS M6 rack servers, the Cisco UCS 15428 VIC adapter remains stuck in the Inoperable state. The server fails to receive discovery from Cisco UCS Manager due to a DHCP packet parsing error at the Baseboard Management Controller (BMC). This error occurs because the DHCP packet contains extra fields or characters, causing Cisco UCS Manager initialization to fail with a `FATAL ERROR! Invalid UCSM DHCP mode token` message and aborting the mode change process. This issue prevents proper adapter operation and server discovery. This issue is resolved.	4.3(6g)	6.0(2d)

Resolved Caveats in Release 6.0(2c)

The following caveats are resolved in release 6.0(2c):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwt35920	Certain RTX Pro 6000 GPUs shipped as spares may experience a firmware update discrepancy. Although the Host Update Utility (HUU) reports that the update has completed successfully, the GPU firmware version on these specific units remains unchanged. This issue is restricted to select spare components and does not impact the standard update process for other hardware. This issue is resolved.	6.0(2b)	6.0(2c)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
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.	4.3(5a)	6.0(2c)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
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.	6.0(2b)	6.0(2c)
CSCwt45410	During the infrastructure (A Bundle) upgrade from releases 4.3(6) or 6.0(1) to 6.0(2), the AES encryption key is deleted. This causes MACsec sessions using Type-6 keys in must secure mode to go down, resulting in traffic loss. The major fault message Primary Encryption key has not been set for MACsec keys is raised. This issue is resolved.	6.0(2b)	6.0(2c)

Resolved Caveats in Release 6.0(2b)

The following caveats are resolved in release 6.0(2b):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwt36346	On Cisco UCS 6500 Series and 6400 Series Fabric Interconnects, when the allowed VLAN string on the vEth interface exceeds 900 characters, data corruption occurs over time. This eventually causes both Fabric Interconnects to perform a hard reboot. The generic error message Reset Requested due to Fatal Module Error is displayed when the show system reset-reason command is run. This issue is resolved.	6.0(1b)	6.0(2b)
CSCwq30478	The Fabric Interconnects (FI) svc_samc_proxy process may repeatedly log **dead thread** messages in the proxy log. Despite these messages, communication continues without interruption. This issue is resolved.	4.2(3g)A	6.0(2b)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCws62117	Cisco UCS C240-M8 server with LPe35002-M2 Emulex adapters connected to Brocade SAN switches and Dell storage arrays experience intermittent I_T Nexus Loss 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(6c)	6.0(2b)
CSCwr51315	NVMe drives UCS-NVMEG4-M7680 with firmware E2CS005 in Cisco UCS-X blade servers 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(1c)	6.0(2b)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwq80370	The PSU firmware version reported under the PowerSubsystem in Redfish API on Cisco UCS X chassis may show incorrect or inconsistent values compared to the FirmwareInventory or PSUFWUPDATE information. This discrepancy can occur after an Embedded Service Update, where the Redfish interface displays outdated or partial firmware versions, while the actual primary and secondary firmware versions differ. This issue is resolved.	6.0(1d)	6.0(2b)
CSCwr73352	Multiple Cisco X210c M7 servers experience Cisco IMC reboots triggered by BMC watchdog hard resets. This causes service profiles to become inaccessible temporarily. This behavior may impact server management availability during the reset events. This issue is resolved.	6.0(1d)	6.0(2b)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCws91466	IOMs in the Cisco UCS domain running Cisco UCS Manager version report a CMCLowMem warning related to high usage of the /var/volatile/wtmp file, which grows due to repeated FI connections triggering rlogin. The wtmp file consumes about 1.4 GB of space, but no other service impact is observed. This issue is resolved.	4.3(6b)A	6.0(2b)A
CSCwq95692	When a VLAN is deleted from a VLAN Group assigned to a vNIC in a Service Profile that is in a **pending reboot** state with a **user-ack** maintenance policy, uplink configuration changes do not apply in NXOS. Service Profiles remain in **pending reboot** and require user acknowledgment, causing potential network connectivity problems due to incomplete VLAN configurations. This scenario affects Service Profiles Profiles associated with servers after Host Firmware Package changes. This issue is resolved.	4.2(3l)A	6.0(2b)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwr55882	After a Cisco UCS Manager upgrade, fabric evacuation on IOM backplane ports may not turn off because some servers remain in a shallow discovery state. This causes affected backplane ports to stay down, while others in the domain may come up normally. The issue typically occurs when fabric evacuation is manually enabled before the upgrade and after the first Fabric Interconnect completes the upgrade. This issue is resolved.	4.3(5c)	6.0(2b)
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(5c)	6.0(2b)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwr02103	After upgrading to Cisco UCS Manager, NVMe drives may become unavailable due to a storage controller fault. The storage controllers show as inoperable with fault code F1004, indicating missing catalog support. This issue causes the impacted NVMe drives to become unresponsive and unavailable. This issue is resolved.	4.3(5c)	6.0(2b)
CSCwr64103	After upgrading the infrastructure bundle to 4.3(6c) or later, CLI access to FI management IPs may be blocked due to a session limit error stating **More than 32 UCSM CLI sessions are not allowed**. LDAP and local admin SSH logins fail, but web GUI access remains unaffected. Primary FI logs may show corrupted **sam_techsupportinfo** files with Cisco UCS Manager information errors. This issue is resolved.	4.3(5a)	6.0(2b)
CSCws40268	The SAS Expander tab is missing in Cisco UCS Manager GUI for C240 M5 servers with SAS Expanders connected to HBAs. Drives remain visible at the OS and in logs, and Cisco IMC shows the SAS Expander as operational. This issue is resolved.	4.3(5a)	6.0(2b)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwt11034	Cisco UCS 6400 series FIs show a warning about missing identity files and prompt for a user password when remote users connect to the peer fabric NXOS. The warning indicates that the SSH identity file is not accessible. This issue is resolved.	6.0(1f)	6.0(2b)
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.	4.3(6f)	6.0(2b)

Resolved Caveats in Release 6.0(1h)

The following caveats are resolved in release 6.0(1h):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwt36346	On Cisco UCS 6500 Series and 6400 Series Fabric Interconnects, when the allowed VLAN string on the vEth interface exceeds 900 characters, data corruption occurs over time. This eventually causes both Fabric Interconnects to perform a hard reboot. The generic error message Reset Requested due to Fatal Module Error is displayed when the show system reset-reason command is run. This issue is resolved.	6.0(1b)	6.0(1h)
CSCwn65484	Cisco UCS Fabric Interconnects (6400, 6500, 6600 Series, and Cisco UCS X-Series Direct UCS 9108 100G) may generate a missing FCOE_NPV_PKG license warning. The warning message is: %LICMGR-2-LOG_LIC_MISSING_WARNING Despite this warning, the FCoE feature continues to operate normally under honor-based licensing. This issue is resolved.	4.2(3o)	6.0(1h)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwt30293	During the Cisco UCS Manager upgrade, the system validates hardware compatibility. If unsupported hardware is detected, the upgrade validation fails and the process rolls back. In some cases, rollback may not complete successfully, causing one Fabric Interconnect to become unresponsive. This results in loss of redundancy, with only the primary Fabric Interconnect remaining operational. The system maintains stability by preventing cluster disruption during validation failures. This issue is resolved.	6.0(1f)	6.0(1h)

Resolved Caveats in Release 6.0(1f)

The following caveat is resolved in release 6.0(1f):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCws83445	On Cisco UCS 6664 Fabric Interconnects, certain unified ports failed to come up, affecting both Ethernet and Fibre Channel connectivity. This issue occurred on devices reporting a hardware changes bit value of 0x0 in the supervisor SPROM. This issue is resolved.	6.0(1b)	6.0(1f)

Resolved Caveats in Release 6.0(1e)

The following caveats are resolved in release 6.0(1e):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwq03209	Cisco UCS Manager attempts to view SEL logs for blades and rack servers across multiple chassis fail with the error **Software Error: Failed to construct the sel command to execute**. This issue is resolved.	4.3(5c)	6.0(1e)
CSCws30219	Cisco UCS M7 servers managed by Cisco UCS Manager with server bundle versions 4.3(6c), 4.3(6d), 6.0(1b), 6.0(1c), and 6.0(1d) are susceptible to host lockups triggered by ECC (Error Correcting Code) memory events. This issue is specifically related to how the server BIOS interacts with the Extensible Firmware Interface (EFI) 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 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.	4.3(6c) server bundle B/C	6.0(1e) server bundle B/C

Resolved Caveats in Release 6.0(1d)

The following caveats are resolved in release 6.0(1d):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwp91696	On the Cisco UCS X215c M8 Compute Node, when the system boots with all drive slots empty and runs RHEL 9.6, inserting E3.S NVMe drives causes the link speed to drop to Gen 4 instead of Gen 5. This issue occurs only if no drives are present during boot. If at least one drive is installed at boot, the link speed remains at Gen 5. This issue is resolved.	6.0(1b)	6.0(1d)
CSCwq01510	On Cisco UCS servers with AMD Genoa CPUs and the UCSX-X10C-PTE3 Passthrough E3.S storage controller, E3.S NVMe drives in slots 8 and 9 are not detected if those slots are empty when the operating system starts. In Microsoft Windows 2025, adding drives to these slots does not trigger auto-refresh, and in ESXi 8.0U3e, the drives are not detected at all. This issue only occurs if slots 8 and 9 are empty at boot. This issue is resolved.	6.0(1b)	6.0(1d)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwr24516	Cisco UCS blade server encounters a power-on failure and does not boot due to an under-current fault in the standby voltage regulator for CPU1. The fault is identified by the IOUT UC FAULT flag in the voltage regulator fault registers. This issue prevents normal system startup. This issue is resolved.	6.0(1b)	6.0(1d)
CSCwq34720	Re-association of the Cisco UCS X210c M7 compute node, running Windows 2022 Server with Secure Boot enabled, fails with the following error:SBAT self-check failed: Security Policy Violation. This issue is resolved.	4.3(5c)B	6.0(1d)B
CSCwq38681	Cisco UCS Central release 2.0(1w) can delete locally configured Trust Points on Cisco UCS Manager when it is managed by Cisco UCS Central with all settings, including User Management, set to Global. This deletion triggers alarms if keyrings related to the deleted Trust Point exist. This issue is resolved.	4.3(6a)	6.0(1d)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwq94580	After rollback of the infrastructure bundle to version 6.0(1b), all Cisco UCS M5 rack servers experience discovery and service profile disassociation failures due to **Setup of Vmedia failed**. This issue occurs in domains with Cisco UCS FI 6400, 6536, and UCSX-S9108-100G when unsupported hardware or software configurations are present. This issue is resolved.	6.0(1b)	6.0(1d)

Resolved Caveats in Release 6.0(1c)

Defect ID	Symptom	First Bundle 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.	6.0(1b)	6.0(1c)

Resolved Caveats in Release 6.0(1b)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwo62993	Secure LDAP authentication fails intermittently on some Cisco UCS Manager domains after trustpoint configuration changes. The issue manifests as **TLS start failed** errors and **unknown CA** alerts, indicating certificate validation problems. Affected domains show **unable to get local issuer certificate** errors during SSL verification despite network connectivity to the LDAP server. This issue is resolved.	4.3(3a)	6.0(1b)
CSCwp64077	The snmpd process on Cisco UCS FI experiences recurring crashes triggered by kernel messages **sap recovering failed and so Killed with SIGABRT - kernel.** This crash can occur when querying OID's of BRIDGE-MIB [OID starting with 1.3.6.1.2.1.17]. This issue is resolved.	4.3(5a)A	6.0(1b)A
CSCwi16863	A watchdog reset causes the BMC to perform a hard reset on the Cisco UCS B200 M6 or X210c M6 servers and FI with infra version 4.2(3d). The reset is logged with system event messages indicating the Cisco IMC reboot due to the watchdog reset assertion. This issue is resolved.	4.2(3d)	6.0(1b)A

Open Caveats

Open Caveats in Release 6.0(2e)

There are no new open caveats in release 6.0(2e).

Open Caveats in Release 6.0(2d)

There are no new open caveats in release 6.0(2d).

Open Caveats in Release 6.0(2c)

The following caveat is open in release 6.0(2c):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCws49799	In certain scenarios involving drive hot-plug and VM lifecycle operations, NVMe drives may appear as degraded in the out-of-band (OOB) management interface despite) management interface despite showing no errors on the host and functioning normally within the VM. This condition can persist even after drives are removed, reseated, and reassigned.	There is no known workaround.	6.0(2b)
CSCwt98100	In UCS X-Series Direct, downgrading from release 6.0(2c) with AES encryption enabled to any 4.3(4a) patch release is not supported. AES encryption must be enabled in 6.0(2c) for this issue to occur, and there is no option to disable AES encryption in this release. Attempts to downgrade under these conditions fail with an error indicating the downgrade path is unsupported.	There is no known workaround.	6.0(2c)

Open Caveats in Release 6.0(2b)

The following caveats are open in Release 6.0(2b):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwt14361	Remote authentication login using TACACS fails on a Fabric Interconnect (FI) after the UCS domain FI IP address changes following the initial certificate installation with the original Cisco UCS Manager domain IPs. Although the TACACS configuration is successfully pushed to the FI, remote login via TACACS to the affected FI fails, while LDAP login continues to work on all FIs. This issue occurs because the initial certificate was generated using the IP address of the FI instead of the hostname, and the IP address of the FI has since changed. Remote authenticated users should be able to log in to all FI IP addresses, including the newly joined secondary FI, but this failure prevents TACACS login on the secondary FI after the IP change.	1. When the FI IP address changes, obtain a new certificate reflecting the updated IP. If DNS names are used instead of IP addresses, certificate regeneration is not required. 2. On the Cisco Identity Services Engine server (ISE), enable additional attribute checks such as DNS verification as recommended by Cisco ISE software to enhance authentication reliability.	6.0(2b)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwt45410	During the infrastructure (A Bundle) upgrade from releases 4.3(6) or 6.0(1) to 6.0(2), the AES encryption key is deleted. This causes MACsec sessions using Type-6 keys in must secure mode to go down, resulting in traffic loss. The major fault message `Primary Encryption key has not been set for MACsec keys` is raised.	Before acknowledging the reboot of the primary Fabric Interconnect during the infrastructure bundle upgrade, configure the primary encryption key. Perform the following steps: 1. Enter the security scope:**UCS# scope security** 2. Enter the encryption scope: **UCS# /security # scope encryption** 3. Set the encryption key:**UCS# /security/encryption # set encryption-key** **Enter the Encryption Key:** **Confirm the Encryption Key:** 4. Commit the changes:**UCS# /security/encryption* # commit-buffer** After configuring the key, verify that the MACsec session and statistics on the secondary Fabric Interconnect are normal. Then proceed to acknowledge the reboot of the primary Fabric Interconnect.	6.0(2b)

Defect ID	Symptom	Workaround	First Bundle Affected
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 work around. 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(2b)
CSCwt15440	Fabric Interconnect (FI) ports using 64G Fibre Channel (FC) SFPs may experience incrementing input discards and errors, leading to errDisabled state due to high bit error rates when configured at 16G speed in FC Switch mode. Additionally, FC Name Server (FCNS) entries for targets connected to MDS switches may show empty vendor names on the FI. This issue occurs when FC ports on Cisco UCS FI 6652 use 64G FC SFPs but are set to operate at 16G speed while sending FCoE traffic across multiple VSANs.	Use 16G or 32G SFP	6.0(2b)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwt35920	Certain RTX Pro 6000 GPUs shipped as spares may experience a firmware update discrepancy. Although the Host Update Utility (HUU) reports that the update has completed successfully, the GPU firmware version on these specific units remains unchanged. This issue is restricted to select spare components and does not impact the standard update process for other hardware.	There is no known workaround.	6.0(2b)

Open Caveats in Release 6.0(1h)

There are no new open caveats in release 6.0(1h).

Open Caveats in Release 6.0(1f)

There are no new open caveats in release 6.0(1f).

Open Caveats in Release 6.0(1e)

There are no new open caveats in release 6.0(1e).

Open Caveats in Release 6.0(1d)

There are no new open caveats in release 6.0(1d).

Open Caveats in Release 6.0(1c)

There are no new open caveats in release 6.0(1c).

Open Caveats in Release 6.0(1b)

The following caveats are open in Release 6.0(1b).

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwt36346	On Cisco UCS 6500 Series and 6400 Series Fabric Interconnects, when the allowed VLAN string on the vEth interface exceeds 900 characters, data corruption occurs over time. This eventually causes both Fabric Interconnects to perform a hard reboot. The generic error message Reset Requested due to Fatal Module Error is displayed when the show system reset-reason command is run.	Configure all vEth interfaces so that their allowed VLAN string length is 900 characters or less.	6.0(1b)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCws30219	Cisco UCS M7 servers managed by Cisco UCS Manager with server bundle versions 4.3(6c), 4.3(6d), 6.0(1b), 6.0(1c), and 6.0(1d) are susceptible to host lockups triggered by ECC (Error Correcting Code) memory events. This issue is specifically related to how the server BIOS interacts with the Extensible Firmware Interface (EFI) 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 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 the server bundle to release 4.3(6b) or an earlier server bundle.	4.3(6c) server bundle B/C

Defect ID	Symptom	Workaround	First Bundle 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 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.	Install the OS on drive configured in RAID.	4.3(6a)
CSCwq34720	Re-association of the Cisco UCS X210c M7 compute node, running Windows 2022 Server with **Secure Boot** enabled, fails with the following error:`SBAT self-check failed: Security Policy Violation`	Remove the SBAT variable from the BIOS token and then perform a CMOS clear. After this, the service profile association will complete successfully with Secure Boot enabled, allowing the system to boot normally. Cisco recommends that you contact TAC for further assistance.	4.3(5c)B

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwq94580	After upgrading the infrastructure A bundle to release 6.0(1b), server maintenance operations on Cisco UCS C Series M5 rack servers may fail due to unsupported hardware or software configurations detected during the upgrade. This issue occurs in setups equipped with Cisco UCS FI models 6400 series, 6536, and UCSX-S9108-100G.	You must reboot the FIs sequentially starting with secondary role FI first. **Note** Rebooting the FIs is a disruptive operation that will result in a temporary service interruption. It is recommended to perform this task during a planned maintenance window. Cisco recommends that you contact TAC for further assistance.	6.0(1b)
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.	There is no known workaround.	4.3(5a)

Known Behavior and Limitations

Known Behavior and Limitations in Release 6.0(2e)

There are no new know limitations in release 6.0(2e).

Known Behavior and Limitations in Release 6.0(2d)

There are no new know limitations in release 6.0(2d).

Known Behavior and Limitations in Release 6.0(2c)

There are no new know limitations in release 6.0(2c).

Known Behavior and Limitations in Release 6.0(2b)

There are no new know limitations in release 6.0(2b).

Known Behavior and Limitations in Release 6.0(1h)

There are no new know limitations in release 6.0(1h).

Known Behavior and Limitations in Release 6.0(1f)

There are no new know limitations in release 6.0(1f).

Known Behavior and Limitations in Release 6.0(1e)

There are no new know limitations in release 6.0(1e).

Known Behavior and Limitations in Release 6.0(1d)

There are no new know limitations in release 6.0(1d).

Known Behavior and Limitations in Release 6.0(1c)

There are no new know limitations in release 6.0(1c).

Known Behavior and Limitations in Release 6.0(1b)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwq41000	Broadcom AERO RAID controller (UCSX-X10C-RAIDF) for Cisco UCS X210c server and Cisco 12G Modular Raid controller with 4GB Cache (UCSC-RAID-M6T) do not transition drives from **Unconfigured Good (UG)** to **Online** state when **Auto Configuration Mode (ACM)** is set to RAID0 after storage profile redeploy and server reboot. As a result, RAID0 LUNs are not created. This issue affects drive state transitions and RAID0 LUN creation on Cisco Tri-Mode 24G SAS RAID Controller w/4GB Cache (UCSC-RAID-HP).	There is no known workaround.	6.0(1b)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwm70985	During or immediately after a firmware upgrade/downgrade on NVIDIA L40s GPUs, no read/write operations should be performed on the card. However, PNUOS performs read operations using the nvidia-smi utility to check the GPU mode immediately after the upgrade. This issue occurs when upgrading/downgrading firmware on NVIDIA L40 GPUs, causing PNUOS to crash and raise a major fault. As a result, Cisco UCS Manager does not support mode switch for NVIDIA L40 GPUs from release 4.3(5a) onwards.	You can perform mode changes using NVIDIA tools on the host OS if required. This limitation does not affect other L-series GPUs, which continue to support mode changes.	4.3(5a)

Compatibility

Cisco UCS Manager and Cisco UCS C-Series Release Compatibility Matrix for C-Series Rack-Mount Servers

Cisco UCS C-Series Rack-Mount Servers are managed by built-in standalone software— Cisco Integrated Management Controller (Cisco IMC). However, when a C-Series Rack-Mount Server is integrated with Cisco UCS Manager, the Cisco IMC does not manage the server anymore.

Each Cisco UCS Manager release incorporates its corresponding C-Series Standalone release. For example, Cisco UCS Manager Release 4.3(6) includes the 4.3(6) server bundle for all the M8, M7, M6 and S3260 M5 servers, and the 4.3(2) server bundle for all other M5 servers. This ensures support for all M8, M7, M6, and M5 servers listed in the C-Series Standalone releases.

Cisco UCS Equivalency Matrix for Cisco Intersight, Cisco IMC, and Cisco UCS Manager outlines the release timeline for Cisco Intersight, Cisco Integrated Management Controller (IMC), and Cisco UCS Manager (UCSM). It includes essential information such as the date each patch was posted, the specific patch version, and the platforms that are supported by each release. By referring to this matrix, you can identify the appropriate firmware and software versions required for your servers before migrating them to Cisco Intersight. This ensures that your server infrastructure remains supported and operates efficiently during and after the transition.

The following table lists the Cisco UCS Manager and C-Series software standalone releases for C-Series Rack-Mount Servers:

Table 3: Cisco UCS Manager and C-Series Software releases for C-Series Servers

Cisco UCS Manager Release	C-Series Standalone Releases Included	C-Series Servers Supported by the C-Series Standalone Releases
6.0(2)	6.0(2)	All M8, M7, M6, and S3260 M5
	4.3(2)	All M5
6.0(1)	6.0(1)	All M8, M7, M6, and S3260 M5
	4.3(2)	All M5
4.3(6)	4.3(6)	All M8, M7, M6, and S3260 M5
	4.3(2)	All M5
4.3(5)	4.3(5)	All M8, M7, and M6
	4.3(4)	S3260 M5
	4.3(2)	All M5
4.3(4)	4.3(4)	C245 M8 All M7, M6, and S3260 M5
	4.3(2)	All M5
4.3(3)	4.3(3)	All M7, M6, and S3260 M5
	4.3(2)	All M5
4.3(2)	4.3(2)	All M7, M6, and M5
4.2(3)	4.2(3)	All M6, M5, and S3260 M4
	4.1(3)	All M5 and S3260 M4
	4.1(2)	C220 M4, C240 M4, and C460 M4
4.2(2)	4.2(2)	All M6, M5, and S3260 M4
	4.1(3)	S3260 M4, All M5
	4.1(2)	C220 M4, C240 M4, C460 M4
4.2(1)	4.2(1)	All M6
	4.1(3)	S3260 M4, All M5
	4.1(2)	C220 M4, C240 M4, C460 M4

Cisco UCS Manager Release	C-Series Standalone Releases Included	C-Series Servers Supported by the C-Series Standalone Releases
4.1(3)	4.1(3)	S3260 M4, All M5
	4.1(2)	C220 M4, C240 M4, C460 M4
	3.0(4)	All M3
4.1(2)	4.1(2)	C220 M5, C240 M5, C240 SD M5, C480 M5, S3260 M5, C480 M5 ML, C125 M5, C220 M4, C240 M4, C460 M4, S3260 M4
	3.0(4)	All M3
4.1(1)	4.1(1)	C220 M5, C240 M5, C480 M5, S3260 M5, C125 M5, C480 M5 ML only
	4.0(2)	C220 M4, C240 M4, C460 M4, S3260 M4, C125 M5 only
	3.0(4)	All M3
4.0(4)	4.0(4)	C220 M5, C240 M5, C480 M5, S3260 M5, C480 M5 ML only
	4.0(2)	C220 M4, C240 M4, C460 M4, S3260 M4, C125 M5 only
	3.0(4)	All M3
4.0(2)	4.0(2)	C220 M4, C240 M4, C460 M4, C220 M5, C240 M5, C480 M5, S3260 M4, S3260 M5, C125 M5, C480 M5 ML only
	3.0(4)	All M3
4.0(1)	4.0(1)	C220 M4, C240 M4, C460 M4, C220 M5, C240 M5, C480 M5, S3260 M4, S3260 M5, C125 M5 only
	3.0(4)	All M3

Cross-Version Firmware Support

The Cisco UCS Manager A bundle software (Cisco UCS Manager, Cisco NX-OS, IOM and FEX firmware) can be mixed with previous B or C bundle releases on the servers (host firmware [FW], BIOS, Cisco IMC, adapter FW and drivers). To help you quickly verify valid combinations, this release includes an interactive compatibility tool, available here:

Cisco UCS Manager Cross Version Firmware Matrix

By selecting a Fabric Interconnect model along with the desired Infrastructure (A Bundle) and Host Firmware (B and C Bundles) releases, the tool dynamically displays whether each combination is a supported configuration.



Note Beginning with Cisco UCS Manager Release 6.0(1b), Cisco UCS 6300 Series FI and Cisco UCS 6332 FI are not supported.

Table 4: Mixed Cisco UCS Releases Supported on Cisco UCS 6652, 6664, 6536, and 6400 series Fabric Interconnects

	Infrastructure Versions (A Bundles)									
Host FW Versions (B or C Bundles)	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)	—	—	—	—	—	—	—	—	6664, 6536, 6454, 64108	6652, 6664, 6536, 6454, 64108
6.0(1)	—	—	—	—	—	—	—	—	6664, 6536, 6454, 64108	6664, 6536, 6454, 64108
4.3(6)	—	—	—	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6536, 6454, 64108	6536, 6454, 64108
4.3(5)	—	—	—	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6536, 6454, 64108	6536, 6454, 64108
4.3(4)	—	—	—	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6536, 6454, 64108	6536, 6454, 64108
4.3(3)	—	—	—	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6536, 6454, 64108	6536, 6454, 64108

	Infrastructure Versions (A Bundles)									
4.3(2)	—	—	—	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6536, 6454, 64108	6536, 6454, 64108
4.2(3)	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	6536, 6454, 64108	6536, 6454, 64108
4.2(2)	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108	6332, 6332-16UP, 6454, 64108	6332, 6332-16UP, 6454, 64108	6332, 6332-16UP, 6454, 64108	6332, 6332-16UP, 6454, 64108	6332, 6332-16UP, 6454, 64108	—	—
4.2(1)	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108	6332, 6332-16UP, 6454, 64108	6332, 6332-16UP, 6454, 64108	6332, 6332-16UP, 6454, 64108	6332, 6332-16UP, 6454, 64108	6332, 6332-16UP, 6454, 64108	—	—

Table 5: Mixed Cisco UCS Releases Supported on Cisco UCS X-Series Direct

Host FW Versions (B and C Bundles)	Infrastructure Versions (A Bundles)				
Note **Cisco UCS X-Series Direct supports Cisco UCS C-Series servers starting from release 6.0(1).** **Extended Chassis UCS X9508 is supported from release 6.0(1b) onwards.**					
	4.3(4)	4.3(5)	4.3(6)	6.0(1)	6.0(2)
6.0(2)	—	—	—	UCSX-S9108-100G	UCSX-S9108-100G
6.0(1)	—	—	—	UCSX-S9108-100G	UCSX-S9108-100G
4.3(6)	UCSX-S9108-100G	UCSX-S9108-100G	UCSX-S9108-100G	—	—
4.3(5)	UCSX-S9108-100G	UCSX-S9108-100G	UCSX-S9108-100G	—	—
4.3(4)	UCSX-S9108-100G	UCSX-S9108-100G	UCSX-S9108-100G	—	—

You may also view the extended version of the Mixed Cisco UCS Releases Supported on Cisco UCS Fabric Interconnects at Cisco UCS Manager Cross-Version Firmware Support 6.0.

For reference, the Cisco UCS Equivalency Matrix for Cisco Intersight, Cisco IMC, and Cisco UCS Manager outlines the release timeline for Cisco Intersight, Cisco Integrated Management Controller (Cisco IMC), and Cisco UCS Manager. It includes essential information such as the date each patch was posted, the specific patch version, and the platforms that are supported by each release. By referring to this matrix, you can identify the appropriate firmware and software versions required for your servers before migrating them to Cisco Intersight. This ensures that your server infrastructure remains supported and operates efficiently during and after the transition.

Upgrade and Downgrade Guidelines

To get a complete overview of all the possible upgrade paths in Cisco UCS Manager, see Cisco UCS Manager Upgrade/Downgrade Support Matrix.

Upgrade and Downgrade to Release 6.0(2)

- After downgrading from release 6.0(2) to 6.0(1) or any lower version, the **Support Host Key RSA** key size remains at 4096 bits and does not revert to 2048 bits unless a Fabric Interconnect (FI) reboot with **erase config** is performed; this is expected system behavior and should be considered during upgrade or downgrade planning.
- Before downgrading from Release 6.0(2) to an earlier version, ensure that all security faults related to **Unencrypted Traffic** or **Insecure Configurations** are resolved and cleared in 6.0(2). Any such faults present during downgrade may persist in the earlier version and cannot be cleared, as previous releases do not support the necessary configuration options.
- Starting with Cisco UCS Manager Release 6.0(2), SHA 512 is the recommended authentication protocol for secure SNMP communication. The MD5 and SHA authentication options remain in the user interface for backward compatibility to support upgrade or downgrade scenarios. However, the use of MD5 or SHA results in system faults and prevent user deployment in this release.

Table 6: Upgrade Paths to Release 6.0(2)

Upgrade from Release	Recommended Upgrade Path
Upgrade from any 6.0(1) release	Direct upgrade or downgrade to release 6.0(2).
Upgrade from any 4.3(6) release	Direct upgrade or downgrade to release 6.0(2).
Upgrade from any 4.3(5) release	Direct upgrade or downgrade to release 6.0(2).
Upgrade from any 4.3(4) release	Direct upgrade to release 6.0(2). Downgrade: 1. First downgrade from release 6.0(2) to release 4.3(5). 2. Downgrade to release 4.3(4).

Upgrade from Release	Recommended Upgrade Path
Upgrade from any 4.3(3) release	Direct upgrade to release 6.0(2). Downgrade: 1. First downgrade from release 6.0(2) to release 4.3(5). 2. Downgrade to release 4.3(3).
Upgrade from any 4.3(2) release	Direct upgrade to release 6.0(2). Downgrade: 1. First downgrade from release 6.0(2) to release 4.3(5). 2. Downgrade to release 4.3(2).
Upgrade from any 4.2(3) release	Direct upgrade to release 6.0(2). Downgrade: 1. First downgrade from release 6.0(2) to release 4.3(5). 2. Downgrade to release 4.2(3).
Any other older release	Upgrade: 1. Upgrade to the latest patch of 4.2(3) release. **Note** Refer Release Notes for Cisco UCS Manager, Release 4.2 to identify the recommended upgrade path to release 4.2(3). 2. Download and upgrade to release 6.0(2). Downgrade: 1. First downgrade from release 6.0(2) to release 4.3(5). 2. Downgrade to any other older release. **Note** Refer to the Cisco UCS Manager Release Notes for the specific version you plan to downgrade to.

Upgrade and Downgrade to Release 6.0(1)

- If your setup is equipped with Cisco UCS 6664 Fabric Interconnect, you cannot downgrade Infrastructure Firmware Version (A Bundle) to any release earlier than 6.0(1b).

- If your setup is equipped with Cisco UCS X-Series Direct (Fabric Interconnect 9108 100G) and Cisco UCS C-Series rack servers or a secondary chassis, then you cannot downgrade to any release earlier than 6.0(1b).
- If your setup includes Cisco Tri-Mode M1 24G RAID (UCSC-RAID-M1L16) controllers on Cisco UCS C240 M8 Servers, then you can not downgrade to any release earlier than 6.0(1b).
- Once you enable any of the following features, then you cannot downgrade to any release earlier than 6.0(1b). You must first disable these features before downgrading to any earlier release:
  - **Fabric Interconnect Audit Log** support using the Linux Audit Framework (auditd) on Cisco UCS 6600, 6500, or 6400 Series Fabric Interconnects
  - iSCSI boot support using Internet Protocol version 6 (IPv6) for Cisco UCS servers
  - Support for AES master key and MACsec (Type-6 [AES], Type-0, and Type-7 encryption) for Ethernet uplink ports on Cisco UCS 6664 Fabric Interconnects and Cisco UCS X-Series Direct (Cisco UCS Fabric Interconnects 9108 100G)
  - Support for ERSPAN on Cisco UCS X-Series Direct (Cisco UCS Fabric Interconnects 9108 100G)

Table 7: Upgrade Paths to Release 6.0(1)

Upgrade from Release	Recommended Upgrade Path
Upgrade from any 4.3(6) release	Direct upgrade or downgrade to release 6.0(1).
Upgrade from any 4.3(5) release	Direct upgrade or downgrade to release 6.0(1).
Upgrade from any 4.3(4) release	Direct upgrade to release 6.0(1). Downgrade: **1.** First downgrade from release 6.0(1) to release 4.3(5). **2.** Downgrade to release 4.3(4).
Upgrade from any 4.3(3) release	Direct upgrade to release 6.0(1). Downgrade: **1.** First downgrade from release 6.0(1) to release 4.3(5). **2.** Downgrade to release 4.3(3).
Upgrade from any 4.3(2) release	Direct upgrade to release 6.0(1). Downgrade: **1.** First downgrade from release 6.0(1) to release 4.3(5). **2.** Downgrade to release 4.3(2).

Upgrade from Release	Recommended Upgrade Path
Upgrade from any 4.2(3) release	Direct upgrade to release 6.0(1). Downgrade: 1. First downgrade from release 6.0(1) to release 4.3(5). 2. Downgrade to release 4.2(3).
Any other older release	Upgrade: 1. Upgrade to the latest patch of 4.2(3) release. **Note** Refer Release Notes for Cisco UCS Manager, Release 4.2 to identify the recommended upgrade path to release 4.2(3). 2. Download and upgrade to release 6.0(1). Downgrade: 1. First downgrade from release 6.0(1) to release 4.3(5). 2. Downgrade to any other older release. **Note** Refer to the Cisco UCS Manager Release Notes for the specific version you plan to downgrade to.

Internal Dependencies

This section explains the interdependencies between Cisco UCS hardware and Cisco UCS Manager versions, including the following considerations:

- Version dependencies for Server FRU items such as DIMMs depend on the server type.
- Chassis items such as fans and power supplies work with all versions of Cisco UCS Manager.

In this release, an interactive compatibility lookup tool is available to help you quickly determine supported combinations of Infrastructure Releases, Fabric Interconnects, servers, VICs, and IOM modules based on the selected release.

Cisco UCS Manager Internal Dependencies Matrix

Full version of the Internal Dependencies tables is also available for reference: Cisco UCS Manager Internal Dependencies, Release 6.0

Cisco UCS NVMeoF Support Matrix for 3rd Party Storage Vendors

Table 8: Cisco UCS NVMeoF Support Matrix for 3rd Party Storage Vendors

Storage Vendor	Feature	Storage Array	Cisco UCS FI	Cisco UCS VIC	Operating System
NetApp Inc.®	NVMe-FC	ONTAP 9.16 onwards	Cisco UCS 6664 FI, Cisco UCS 6652 FI	15000, 14000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+
		ONTAP 9.15 onwards	Cisco UCS 6400 series, Cisco UCS 6536 FI	1400/14000, 15000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+
		ONTAP 9.15 onwards	Cisco UCS X-Direct	15000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+
	NVMe-TCP	ONTAP 9.16 onwards	Cisco UCS 6664 FI, Cisco UCS 6652 FI	15000, 14000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+
		ONTAP 9.15 onwards	Cisco UCS 6400 series, Cisco UCS 6536 FI	1400/14000/15000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+
		ONTAP 9.15 onwards	Cisco UCS X-Direct	15000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+

Note
Refer https://hwu.netapp.com/ for latest Storage Array support details.

A valid NetApp® account is required to access the compatibility information.

Storage Vendor	Feature	Storage Array	Cisco UCS FI	Cisco UCS VIC	Operating System
Pure Storage, Inc.®	NVMe-FC	FlashArray//C, FlashArray//X, FlashArray//XL	Cisco UCS 6652 FI Cisco UCS 6664 FI	15000, 14000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+
		FlashArray//C, FlashArray//X, FlashArray//XL	Cisco UCS 6400 series, Cisco UCS 6536 FI	1400/14000, 15000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+
		FlashArray//C, FlashArray//X, FlashArray//XL	Cisco UCS X-Direct	15000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+
	NVMe-ROCEv2	FlashArray//C, FlashArray//X, FlashArray//XL	Cisco UCS 6652 FI	15000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+
		FlashArray//C, FlashArray//X, FlashArray//XL	Cisco UCS 6664 FI	15000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+
		FlashArray//C, FlashArray//X, FlashArray//XL	Cisco UCS 6400 series, Cisco UCS 6536 FI	15000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+
		FlashArray//C, FlashArray//X, FlashArray//XL	Cisco UCS X-Direct	15000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+
	NVMe-TCP	FlashArray//C, FlashArray//X, FlashArray//XL	Cisco UCS 6652 FI	15000, 14000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+
		FlashArray//C, FlashArray//X, FlashArray//XL	Cisco UCS 6664 FI	15000, 14000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+

Storage Vendor	Feature	Storage Array	Cisco UCS FI	Cisco UCS VIC	Operating System
		FlashArray//C, FlashArray//X, FlashArray//XL	Cisco UCS 6400 series, Cisco UCS 6536 FI	1400/14000, 15000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+
		FlashArray//C, FlashArray//X, FlashArray//XL	Cisco UCS X-Direct	15000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+
Dell Inc.®	NVMe-FC	PowerStore, PowerMax	Cisco UCS 6664 FI, Cisco UCS 6652 FI	15000, 14000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+
		PowerStore, PowerMax	Cisco UCS 6400 series, Cisco UCS 6536 FI	1400/14000, 15000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+
		PowerStore, PowerMax	Cisco UCS X-Direct	15000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+
	NVMe-TCP	PowerStore, PowerMax	Cisco UCS 6664 FI, Cisco UCS 6652 FI	15000, 14000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+
		PowerStore, PowerMax	Cisco UCS 6400 series, Cisco UCS 6536 FI	1400/14000, 15000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+
		PowerStore, PowerMax	Cisco UCS X-Direct	15000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+

Storage Vendor	Feature	Storage Array	Cisco UCS FI	Cisco UCS VIC	Operating System
Hitachi, Ltd. ®	NVMe-TCP	Hitachi VSP One Block 85	UCSX S9108 (EHM)	15000	ESXI 9.0+
	NVMe-TCP	Hitachi VSP One Block 24			
	NVMe-TCP	Hitachi VSP One Block 26			
	NVMe-TCP	Hitachi VSP One Block 28			

Note + under **OS Support** column refers to the newer release in that release train.

Cisco UCS FI Appliance Port Support Matrix

Table 9: Cisco UCS FI Appliance Port Support Matrix

Protocol	Vendor	Partner Support	Cisco Support
Nvme-TCP	NetApp Inc.® (ONTAP)	Supported	Supported
	DELL EMC®	Supported	Supported
	Pure Storage Inc.®	Supported	Supported
RoceV2	NetApp Inc.® (ONTAP)	Not supported	Not supported
	DELL EMC®	Not supported	Not supported
	Pure Storage Inc.®	Not supported	Not supported
ISCSI	NetApp Inc.® (ONTAP)	Supported	Supported
	DELL EMC®	Supported	Supported
	Pure Storage Inc.®	Supported	Supported

Cisco UCS Fabric Interconnect and Switch Compatibility Matrix

Compatibility and Support Matrix for Cisco Fabric Interconnects and MDS Switches

Table 10: Cisco UCS Fabric Interconnect and MDS Release Support Matrix

Fabric Interconnect	Older Supported Release of MDS	Recommended release of MDS
Cisco UCS 6652 FI	NA	9.4

Fabric Interconnect	Older Supported Release of MDS	Recommended release of MDS
Cisco UCS 6664 FI	9.2	9.4
Cisco UCS 6536 FI	9.2	9.4
Cisco UCS 6454 FI	9.2	9.4
Cisco UCS 64108 FI	9.2	9.4
Cisco UCS X-Series Direct	9.2	9.4



Note For older supported release only MDS recommended minor version are supported. See Recommended Releases for Cisco MDS 9000 Series Switches for more information.

Compatibility and Support Matrix for Cisco Fabric Interconnects and Nexus Switches

Table 11: Compatibility and Support Matrix for Cisco Fabric Interconnects & Nexus Switches

Fabric Interconnect	Older Supported Release of NX-OS	Recommended release of NX-OS
Cisco UCS 6652 FI	NA	10.6(x)
Cisco UCS 6664 FI	10.5(x)	10.6(x)
Cisco UCS 6536 FI	10.5(x)	10.6(x)
Cisco UCS 6454 FI	10.5(x)	10.6(x)
Cisco UCS 64108 FI	10.5(x)	10.6(x)
Cisco UCS X-Series Direct	10.5(x)	10.6(x)

Compatibility and Support Matrix for Cisco Fabric Interconnects and Brocade Switches

Table 12: Cisco UCS Fabric Interconnect and Brocade Release Support Matrix

Cisco UCS Fabric Interconnect	Older Supported Release of Brocade	Recommended Release of Brocade G620, G630, and X6	Recommended Release of Brocade G720, G730, and X7
Cisco UCS 6652 FI	NA	9.2	10.0
Cisco UCS 6664 FI	9.2	9.2	10.0
Cisco UCS 6536 FI	9.2	9.2	10.0
Cisco UCS 6454 FI	9.2	9.2	10.0
Cisco UCS 64108 FI	9.2	9.2	10.0

Cisco UCS Fabric Interconnect	Older Supported Release of Brocade	Recommended Release of Brocade G620, G630, and X6	Recommended Release of Brocade G720, G730, and X7
Cisco UCS X-Series Direct	9.2	9.2	10.0

Supported Hardware and Software

Supported Operating Systems

For detailed information about supported operating system, see the interactive UCS Hardware and Software Compatibility matrix.

Supported Web Browsers

To access the Cisco UCS Manager GUI, Cisco recommends using the most recent version of one of the following supported browsers for Windows, Linux RHEL, and MacOS:

- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Apple Safari



Note HTML-5 UI supports one user session per browser.

Default Open Ports

The following table lists the default open ports used in Cisco UCS Manager Release 6.0.

Port	Interface	Protocol	Traffic Type	Fabric Interconnect	Usage
22	CLI	SSH	TCP	UCS 6600 Series FI UCS 6400 Series FI UCS 6536 FI UCSX-S9108-100G	Cisco UCS Manager CLI access

Port	Interface	Protocol	Traffic Type	Fabric Interconnect	Usage
80	XML	HTTP	TCP	UCS 6600 Series FI UCS 6400 Series FI UCS 6536 FI UCSX-S9108-100G	Cisco UCS Manager GUI and third party management stations. Client download
443	XML	HTTP	TCP	UCS 6600 Series FI UCS 6400 Series FI UCS 6536 FI UCSX-S9108-100G	Cisco UCS Manager login page access Cisco UCS Manager XML API access
743	KVM	HTTP	TCP	UCS 6600 Series FI UCS 6400 Series FI UCS 6536 FI UCSX-S9108-100G	Cisco IMC Web Service / Direct KVM
7546	CFS	CFSD	TCP	UCS 6600 Series FI UCS 6400 Series FI UCS 6536 FI UCSX-S9108-100G	Cisco Fabric Service

Network Requirements

The *Cisco UCS Manager Administration Management Guide, Release 6.0* provides detailed information about configuring the Intersight Device Connector.

Cisco UCS Central Integration

For the complete list of compatible versions of Cisco UCS Central and Cisco UCS Manager, see *Feature Support Matrix* in Release Notes for Cisco UCS Central.

Supported Platforms in this Release

Release 6.0(2b)

The following servers are supported in this release and continue to receive support in subsequent releases within the same release train:

- Cisco UCS X410c M8 Compute Node

Release 6.0(1b)

The following servers are supported in this release and continue to receive support in subsequent releases within the same release train:

- Cisco UCS C240 M8 Server
- Cisco UCS C220 M8 Server
- Cisco UCS C225 M8 Server
- Cisco UCS C245 M8 Server
- Cisco UCS X210c M8 Compute Node
- Cisco UCS X215c M8 Compute Node
- Cisco UCS C240 M7 Server
- Cisco UCS C220 M7 Server
- Cisco UCS X410c M7 Compute Node
- Cisco UCS X210c M7 Compute Node
- Cisco UCS C220 M6 Server
- Cisco UCS C240 M6 Server
- Cisco UCS C245 M6 Server
- Cisco UCS C225 M6 Server
- Cisco UCS B200 M6 Server
- Cisco UCS X210c M6 Compute Node
- Cisco UCS B200 M5 Server
- Cisco UCS B480 M5 Server
- Cisco UCS S3260 M5 Server
- Cisco UCS C220 M5 Server
- Cisco UCS C240 M5 Server
- Cisco UCS C240 SD M5 Server
- Cisco UCS C480 M5 Server
- Cisco UCS C480 M5 ML Server

- Cisco UCS C125 M5 Server

Other Hardware

We recommend that you use the latest software version for all Chassis, Fabric Interconnects, Fabric Extenders, Expansion Modules and Power Supplies. To determine the minimum software version for your mixed environment, see Cross-Version Firmware Support, on page 64. The following is the list of other supported hardware:

Supported Hardware for UCS 6600 Series Fabric Interconnects

Table 13: Supported Hardware for UCS 6600 Series Fabric Interconnects

Type	Details
Chassis	Cisco UCSX-9508 Chassis (For Cisco UCS X-Series Servers) UCSB-5108-AC2 UCSB-5108-DC2
Fabric Interconnects	UCS 6664 FI and UCS 6652 FI
Fabric Extenders	N9K-C93180YC-FX3 UCSX-I-9108-25G or UCSX-I-9108-100G (Supported with Cisco UCS X-Series Servers) UCS-IOM- 2408
Power Supplies	UCS-PSU-6600-AC UCSX-PSU-2800AC (For Cisco UCSX-9508 Chassis)

Supported Hardware for UCS 6500 Series Fabric Interconnects

Table 14: Supported Hardware for UCS 6500 Series Fabric Interconnects

Type	Details
Chassis	UCSB-5108-AC2 UCSB-5108-DC2 Cisco UCSX-9508 Chassis (For Cisco UCS X-Series Servers)
Fabric Interconnects	UCS 6500

Type	Details
Fabric Extenders	93180YC-FX3 (25G server ports) 93180YC-FX3 (10G server ports) 2408 UCSX-I-9108-25G or UCSX-I-9108-100G (Supported with Cisco UCS X-Series Servers)
Power Supplies	UCS-PSU-6536-AC UCSX-PSU-2800AC (For Cisco UCSX-9508 Chassis)

Supported Hardware for UCS 6400 Series Fabric Interconnects

Table 15: Supported Hardware for UCS 6400 Series Fabric Interconnects

Type	Details
Chassis	UCSC-C4200-SFF N20–C6508 UCSB-5108-DC UCSB-5108-AC2 UCSB-5108-DC2 UCSB-5108-HVDC Cisco UCSX-9508 Chassis (For Cisco UCS X-Series Servers)
Fabric Interconnects	UCS 64108 UCS 6454
Fabric Extenders	93180YC-FX3 (25G server ports) 93180YC-FX3 (10G server ports) 2408 UCSX-I-9108-25G
Power Supplies	UCS-PSU-6332-AC UCS-PSU-6332-DC UCS-PSU-64108-AC UCS-PSU-6332-DC

Supported Hardware for Cisco UCS X-Series Direct

Table 16: Supported Hardware for Cisco UCS X-Series Direct

Fabric Interconnects	Minimum Software Version	Suggested Software Version
Cisco UCS 9108-100G	4.3(4b)	6.0(2e)
Extended Chassis UCS X9508	6.0(1b)	6.0(2e)

GB Connector Modules, Transceiver Modules, and Cables

Following is the list of Gb connector modules, transceiver modules, and supported cables:



Note

- Transceiver modules and cables that are supported on a specific Fabric Interconnect are not always supported on all VIC adapters, IOMs, or FEXes that are compatible with that Fabric Interconnect. Detailed compatibility matrices for the transceiver modules are available here:https://www.cisco.com/c/en/us/support/interfaces-modules/transceiver-modules/products-device-support-tables-list.html
- S-Class transceivers, for example, QSFP-40G-SR4-S, do not support FCoE.

Table 17: Cisco UCS 6600 Series Fabric Interconnect

Gb Connector Modules	Transceiver Modules and Cables
FC SFP for UCS 6600 Series Fabric Interconnects	DS-SFP-FC16G-SW DS-SFP-FC32G-SW DS-SFP-FC64G-SW DS-SFP-FC16G-LW DS-SFP-FC32G-LW DS-SFP-FC64G-LW

Gb Connector Modules	Transceiver Modules and Cables
10GbE on Unified Port for UCS 6600 Series Fabric Interconnects	SFP-H10GB-CU1M SFP-H10GB-CU2M SFP-H10GB-CU3M SFP-H10GB-CU5M SFP-H10GB-ACU7M SFP-H10GB-ACU10M SFP-10G-AOC1M SFP-10G-AOC10M SFP-10G-SR SFP-10G-SR-S SFP-10G-LR SFP-10G-LR-S SFP-H10GB-CU1-5M SFP-H10GB-CU2-5M SFP-10G-AOC2M SFP-10G-AOC3M SFP-10G-AOC5M SFP-10G-AOC7M
10GbE on 100G port (with QSA) for UCS 6600 Series Fabric Interconnects	SFP-10G-SR SFP-10G-SR-S SFP-10G-LR SFP-10G-LR-S

Gb Connector Modules	Transceiver Modules and Cables
25GbE on Unified Port for UCS 6600 Series Fabric Interconnects	SFP-25G-SR-S SFP-10/25G-LR-S SFP-10/25G-CSR-S SFP-25G-SL SFP-H25G-CU1M SFP-H25G-CU2M SFP-H25G-CU3M SFP-H25G-CU4M SFP-H25G-CU5M SFP-25G-AOC1M SFP-25G-AOC2M SFP-25G-AOC3M SFP-25G-AOC4M SFP-25G-AOC5M SFP-25G-AOC7M SFP-25G-AOC10M
25GbE on 100G port (with QSA28) for UCS 6600 Series Fabric Interconnects	SFP-25G-SR-S SFP-25G-SL SFP-10/25G-LR-S SFP-10/25G-CSR-S SFP-10/25G-LR-I

Gb Connector Modules	Transceiver Modules and Cables
40GbE for UCS 6600 Series Fabric Interconnects	QSFP-40G-SR4 QSFP-40G-SR4-S QSFP-40G-LR4 QSFP-H40G-CU1M QSFP-H40G-CU3M QSFP-H40G-CU5M QSFP-H40G-ACU7M QSFP-H40G-AOC3M QSFP-H40G-AOC5M QSFP-H40G-AOC7M QSFP-H40G-AOC15M QSFP-H40G-AOC20M QSFP-H40G-AOC25M QSFP-H40G-AOC30M CVR-QSFP-SFP10G QSFP-40G-LR4-S QSFP-40G-SR-BD QSFP-H40G-ACU10M QSFP-H40G-AOC1M QSFP-H40G-AOC2M QSFP-H40G-AOC7M QSFP-H40G-AOC10M QSFP-H40G-AOC15M QSFP-H40G-AOC20M QSFP-H40G-AOC25M QSFP-H40G-CU2M QSFP-H40G-CU3M QSFP-H40G-AOC30M

Gb Connector Modules	Transceiver Modules and Cables
100GbE for UCS 6600 Series Fabric Interconnects	QSFP-100G-SR4-S QSFP-100G-PSM4-S QSFP-100G-SM-SR QSFP-100G-SL4 QSFP-40/100-SRBD QSFP-100G-DR-S QSFP-100G-FR-S QSFP-100G-SR1.2 QSFP-100G-CU1M QSFP-100G-CU2M QSFP-100G-CU3M QSFP-100G-CU5M QSFP-100G-AOC1M QSFP-100G-AOC2M QSFP-100G-AOC3M QSFP-100G-AOC5M QSFP-100G-AOC7M QSFP-100G-AOC10M QSFP-100G-AOC15M QSFP-100G-AOC20M QSFP-100G-AOC25M QSFP-100G-AOC30M QSFP-100G-LR4-S QSFP-100G-LR-S QSFP-100G0-ER4L-S

Gb Connector Modules	Transceiver Modules and Cables
400GbE for UCS 6652 Fabric Interconnects	QDD-400G-FR4-S QDD-400G-DR4-S QDD-400G-LR8-S QDD-4x100G-LR-S QDD-4x100G-FR-S QDD-400G-LR4-S QDD-400G-CU1M QDD-400G-CU2M QDD-400G-CU3M QDD-400G-AOC1M QDD-400G-AOC2M QDD-400G-AOC3M

Table 18: Cisco UCS 6500 Series Fabric Interconnects

Gb Connector Modules	Transceiver Modules and Cables
FC for UCS 6500 Series Fabric Interconnects	DS-SFP-4X32G-SW
1GbE for UCS 6500 Series Fabric Interconnects	GLC-TE (QSA), port 9, 10 GLC-SX-MMD (QSA)
10GbE for UCS 6500 Series Fabric Interconnects	SFP-10G-SR (QSA) SFP-10G-SR-S(QSA) SFP-10G-LR (QSA) SFP-10G-LR-S (QSA) CVR-QSFP-SFP10G SFP-H10GB-CU1M

Gb Connector Modules	Transceiver Modules and Cables
25GbE for UCS 6500 Series Fabric Interconnects	SFP-10/25G-LR-S SFP-10/25G-CSR-S SFP-25G-SL CVR-QSFP28-SFP25G SFP-H25G-CU1M (P1) SFP-H25G-CU2M (P1) SFP-H25GB-CU3M SFP-25G-AOC2M SFP-25G-AOC3M SFP-25G-SR-S

Gb Connector Modules	Transceiver Modules and Cables
40GbE for UCS 6500 Series Fabric Interconnects	QSFP-H40G-AOC1M QSFP-H40G-AOC2M QSFP-H40G-AOC3M QSFP-H40G-AOC5M QSFP-H40G-AOC15M QSFP-H40G-AOC25M QSFP-40G-CU1M QSFP-40G-CU2M QSFP-40G-CU3M QSFP-40G-CU5M QSFP-40G-SR4 QSFP-40G-SR4-S QSFP-40G-CSR4 QSFP-40G-LR4 QSFP-40G-LR4-S QSFP-4SFP10G-CU1M QSFP-4SFP10G-CU3M FET-40G **Note** FET-40G is supported only between FI and IOM/FEX QSFP-40G-ACU10M QSFP-40G-SR-BD QSFP-100G40G-BIDI **Note** QSFP-100G40G-BIDI is supported only on border ports/uplink ports in 40G mode.

Gb Connector Modules	Transceiver Modules and Cables
100GbE for UCS 6500 Series Fabric Interconnects	QSFP-100G-SR1.2 QSFP-100G-SR4-S QSFP-100G-LR4-S QSFP-100G-SM-SR QSFP-100G-SL4 QSFP-40/100-SRBD (or) QSFP-100G40G-BIDI **Note** QSFP-100G40G-BIDI is supported between FI and I9108-100G IOM/N9K-C93180YC-FX3 FEX/border ports in 100G mode. QSFP-100G-CU1M QSFP-100G-CU2M QSFP-100G-CU3M QSFP-100G-CU5M QSFP-4SFP25G-CU1M QSFP-4SFP25G-CU2M QSFP-4SFP25G-CU3M QSFP-4SFP25G-CU5M QSFP-100G-AOC1M QSFP-100G-AOC2M QSFP-100G-AOC3M QSFP-100G-AOC5M QSFP-100G-AOC7M QSFP-100G-AOC10M QSFP-100G-AOC15M QSFP-100G-AOC20M QSFP-100G-AOC25M QSFP-100G-AOC30M QSFP-100G-DR-S QSFP-100G-FR-S

Table 19: Cisco UCS 6400 Series Fabric Interconnects

Gb Connector Modules	Transceiver Modules and Cables
FC for UCS 6400 Series Fabric Interconnects	DS-SFP-FC8G-SW DS-SFP-FC8G-LW DS-SFP-FC16G-SW DS-SFP-FC16G-LW DS-SFP-FC32G-SW DS-SFP-FC32G-LW
100-Gb for UCS 6400 Series Fabric Interconnects	QSFP-100G-SR1.2 QSFP-40/100G-SRBD QSFP-100G-SR4-S QSFP-100G-LR4-S QSFP-100G-SM-SR QSFP-100G-CU1M QSFP-100G-CU2M QSFP-100G-CU3M QSFP-100G-AOC1M QSFP-100G-AOC2M QSFP-100G-AOC3M QSFP-100G-AOC5M QSFP-100G-AOC7M QSFP-100G-AOC10M QSFP-100G-AOC15M QSFP-100G-AOC20M QSFP-100G-AOC25M QSFP-100G-AOC30M QSFP-4SFP25G-CU1M QSFP-4SFP25G-CU2M QSFP-4SFP25G-CU3M QSFP-4SFP25G-CU5M

Gb Connector Modules	Transceiver Modules and Cables
40-Gb for UCS 6400 Series Fabric Interconnects	QSFP-40G-SR4 QSFP-40G-SR4-S QSFP-40G-SR-BD QSFP-40G-LR4 QSFP-40G-LR4-S QSFP-40G-ER4 WSP-Q40GLR4L QSFP-H40G-CU1M QSFP-H40G-CU3M QSFP-H40G-CU5M QSFP-H40G-ACU7M QSFP-H40G-ACU10M QSFP-H40G-AOC1M QSFP-H40G-AOC2M QSFP-H40G-AOC3M QSFP-H40G-AOC5M QSFP-H40G-AOC10M QSFP-H40G-AOC15M QSFP-4SFP10G-CU1M QSFP-4SFP10G-CU3M QSFP-4SFP10G-CU5M QSFP-4X10G-AC7M QSFP-4X10G-AC10M QSFP-4X10G-AOC1M QSFP-4X10G-AOC3M QSFP-4X10G-AOC5M QSFP-4X10G-AOC7M
32-Gb FC for UCS 6454 Fabric Interconnects	DS-SFP-FC32G-SW DS-SFP-FC32G-LW
25-Gb for UCS 6454 Fabric Interconnects	4x25GbE 10M[1]

Gb Connector Modules	Transceiver Modules and Cables
25-Gb for UCS 6400 Series Fabric Interconnects	SFP-25G-SR-S SFP-H25G-CU1M SFP-H25G-CU2M SFP-H25G-CU3M SFP-H25G-CU5M SFP-H25G-AOC1M SFP-H25G-AOC2M SFP-H25G-AOC3M SFP-H25G-AOC5M SFP-H25G-AOC7M SFP-H25G-AOC10M SFP-10/25G-LR-S SFP-10/25G-CSR-S
16-Gb for UCS 6454 Fabric Interconnects	DS-SFP-FC16G-LW DS-SFP-FC16G-SW

Gb Connector Modules	Transceiver Modules and Cables
10-Gb for UCS 6400 Series Fabric Interconnects	SFP-10G-SR SFP-10G-SR-S SFP-10G-LR SFP-10G-LR-S SFP-10G-ER SFP-10G-ER-S SFP-10G-ZR SFP-10G-ZR-S FET-10G **Note** FET-10G is only supported between Fabric Interconnects and IOMs/FEXs. SFP-10G-LRM SFP-H10GB-CU1M SFP-H10GB-CU2M SFP-H10GB-CU3M SFP-H10GB-CU5M SFP-H10GB-ACU7M SFP-H10GB-ACU10M SFP-10G-AOC1M SFP-10G-AOC2M SFP-10G-AOC3M SFP-10G-AOC5M SFP-10G-AOC7M SFP-10G-AOC10M
8-Gb FC for UCS 6400 Series Fabric Interconnects	DS-SFP-FC8G-SW DS-SFP-FC8G-LW
1-Gb for UCS 6400 Series Fabric Interconnects	GLC-TE GLC-SX-MMD SFP-GE-T

[1] Supported from Cisco UCS Manager, Release 4.1(2)

Table 20: Cisco UCS X-Series Direct Supported Gb Connector Modules

Gb Connector Modules	Cables
100-GbE	QSFP-100G-SR4-S QSFP-100G-SR4-S (Breakout) QSFP-100G-LR4-S QSFP-100G-SM-SR QSFP-100G-SL4 QSFP-100G-SL4 (Breakout) QSFP-100G-SR1.2 QSFP-40/100-SRBD QSFP-100G-DR-S QSFP-100G-FR-S QSFP-100G-CU1M QSFP-100G-CU2M QSFP-100G-CU3M QSFP-100G-CU5M QSFP-100G-AOC1M QSFP-100G-AOC2M QSFP-100G-AOC3M QSFP-100G-AOC5M QSFP-100G-AOC7M QSFP-100G-AOC10M QSFP-100G-AOC15M QSFP-100G-AOC20M QSFP-100G-AOC25M QSFP-100G-AOC30M
40GbE	QSFP-40G-SR4 QSFP-40G-SR4 (Breakout) QSFP-40G-SR4-S QSFP-40G-SR4-S (Breakout) QSFP-40G-CSR4 QSFP-40G-CSR4 (Breakout) QSFP-40G-SR-BD

Gb Connector Modules	Cables
4X25GbE	QSFP-4SFP25G-CU1M QSFP-4SFP25G-CU2M QSFP-4SFP25G-CU3M QSFP-4SFP25G-CU5M
4x10GbE	QSFP-4SFP10G-CU1M QSFP-4SFP10G-CU2M QSFP-4SFP10G-CU3M QSFP-4X10G-AOC3M QSFP-4X10G-AOC5M
25GbE via QSA28	SFP-25G-SR-S SFP-10/25G-LR-S SFP-10/25G-CSR-S SFP-25G-SL SFP-H25G-CU1M SFP-H25G-CU2M SFP-H25G-CU3M SFP-H25G-CU5M
10GbE/1GbE via QSA or QSA28	SFP-10G-SR SFP-10G-SR SFP-10G-SR-S SFP-10G-LR (With QSA) SFP-10G-LR SFP-10G-LR-S SFP-10G-LR-S CVR-QSFP-SFP10G+ GLC-T (ports 7, 8) CVR-QSFP-SFP28+ GLC-T (ports 7, 8)
8G, 16G, 32G FC	4x 8G FC breakout with 128G QSF 4x 16G FC breakoutwith 128G QSFP 4x 32G FC breakoutwith 128G QSFP

Supported GPU/GPU PCIe Node

Table 21: Supported GPU/GPU PCIe Node

GPU/GPU PCIe Node	PID	Supported Servers	Minimum Software Version	Suggested Software Version
NVIDIA RTX Pro 6000 GPU 600W 96GB 2-slot FHFL	UCSC-GPU-RTXP6000	Cisco UCS C240 M8	6.0(2b)	6.0(2e)
NVIDIA A16 GPU on X440p: PCIE 250W 4X16GB, FHFL	UCSX-GPU-A16	Cisco UCS X210c M8 (with PCIe Node)	4.3(6a)	6.0(2e)
	UCSC-GPU-A16	Cisco UCSX215c M8 (with PCIe Node)	4.3(5a)	6.0(2e)
AMD MI210 GPU; 300W 64GB, 2 slot FHFL	UCSX-GPU-MI210	Cisco UCS X215c M8	4.3(6a)	6.0(2e)
NVIDIA H100-NVL GPU 400W, 94GB, 2-slot FHFL	UCSX-GPU-H100-NVL	Cisco UCS X210c M8 (with PCIe Node)	4.3(6a)	6.0(2e)
	UCSC-GPU-H100-NVL	Cisco UCS C240 M8	4.3(6a)	6.0(2e)
		Cisco UCS X210c M7 Cisco UCS X215c M8 (with PCIe Node)	4.3(5a)	6.0(2e)
		Cisco UCS C245 M8	4.3(5a)	6.0(2e)
		Cisco UCS C240 M7	4.3(5a)	6.0(2e)
NVIDIA L4-Mezz GPU 70W, 24GB, 1-slot HHHL	UCSX-GPU-L4-Mezz	Cisco UCS X210c M7 Cisco UCS X215c M8	4.3(5a)	6.0(2e)
UCSX-440P-D GPU PCIe Node	UCSX-440P-D	Cisco UCS X210c M7, X210c M6, and X410c M7	4.3(4a)	6.0(2e)

GPU/GPU PCIe Node	PID	Supported Servers	Minimum Software Version	Suggested Software Version
Intel GPU Flex 140, Gen4x8, HHHL, 75W PCIe (Front Mezz)	UCSX-GPU-FLX140MZ	Cisco UCS X210c M7	4.3(2b)	6.0(2e)
Intel GPU Flex 140, Gen4x8, HHHL, 75W PCIe	UCSX-GPU-FLEX140	Cisco UCS X410c M7 and X210c M7 (with PCIe Node)	4.3(4a)	6.0(2e)
	UCSC-GPU-FLEX140	Cisco UCS C220 M7 and C240 M7	4.3(4a)	6.0(2e)
Intel GPU Flex 170, Gen4x16, HHFL, 150W PCIe	UCSX-GPU-FLEX170	Cisco UCS X410c M7 and X210c M7 (with PCIe Node)	4.3(4a)	6.0(2e)
	UCSC-GPU-FLEX170	Cisco UCS C240 M7	4.3(4a)	6.0(2e)
NVIDIA TESLA A16 PCIE 250W 4X16GB	UCSX-GPU-A16-D	Cisco UCS X210c M7 and X210c M6 (with PCIe Node)	4.3(4a)	6.0(2e)
		Cisco UCS X410c M7 (with PCIe Node)	4.3(4a)	6.0(2e)
	UCSC-GPU-A16	Cisco UCS C240 M8	4.3(6a)	6.0(2e)
		Cisco UCS C240 M6	4.2(1d)	6.0(2e)
		Cisco UCS C245 M6	4.2(1i)	6.0(2e)
NVIDIA L4 Tensor Core, 70W, 24GB	UCSX-GPU-L4	Cisco UCS X210c M8 (with PCIe Node)	4.3(6a)	6.0(2e)
		Cisco UCS X210c M7 (with PCIe Node)	4.3(4a)	6.0(2e)
		Cisco UCS X410c M7 (with PCIe Node)	4.3(4a)	6.0(2e)

GPU/GPU PCIe Node	PID	Supported Servers	Minimum Software Version	Suggested Software Version
NVIDIA L40 300W, 48GB wPWR CBL	UCSX-GPU-L40	Cisco UCS X210c M7 (with PCIe Node)	4.3(4a)	6.0(2e)
		Cisco UCS X410c M7 (with PCIe Node)	4.3(4a)	6.0(2e)
	UCSC-GPU-L40	Cisco UCS C240 M7	4.3(2b)	6.0(2e)
		Cisco UCS X215c M8 (with PCIe Node)	4.3(5a)	6.0(2e)
NVIDIA L40S: 350W, 48GB, 2-slot FHFL GPU	UCSX-GPU-L40S	Cisco UCS X210c M8 (with PCIe Node)	4.3(6a)	6.0(2e)
		Cisco UCS X210c M7 (with PCIe Node) Cisco UCS X410c M7 (with PCIe Node)	4.3(4a)	
	UCSC-GPU-L40S	Cisco UCS C240 M8	4.3(6a)	6.0(2e)
		Cisco UCS C240 M7	4.3(4a)	6.0(2e)
		Cisco UCS X215c M8 (with PCIe Node)	4.3(5a)	6.0(2e)

GPU/GPU PCIe Node	PID	Supported Servers	Minimum Software Version	Suggested Software Version
NVIDIA T4 PCIE 75W 16GB	UCSX-GPU-T4-16	Cisco UCS X210c M6 (with PCIe Node)	4.3(4a)	6.0(2e)
	UCSC-GPU-T4-16	Cisco UCS C220 M6	4.3(2b)	6.0(2e)
		Cisco UCS C245 M6	4.2(1f)	6.0(2e)
		Cisco UCS C225 M6	4.2(1l)	6.0(2e)
		Cisco UCS C240 M5, C220 M5, and C480 M5	3.2(3a)	6.0(2e)
		Cisco UCS S3260 M5	3.1(2b)	6.0(2e)
NVIDIA T4 GPU PCIE 75W 16GB, MEZZ form factor (Front Mezz)	UCSX-GPU-T4-MEZZ	Cisco UCS X210c M7 and X210c M6	4.3(2b)	6.0(2e)
NVIDIA Hopper L4 70W, 24GB, 1-slot HHHL	UCSC-GPU-L4M6	Cisco UCS C220 M6, C240 M6	4.3(4a)	6.0(2e)
NVIDIA H100: 350W, 80GB, 2-slot FHFL GPU	UCSX-GPU-H100-80	Cisco UCS X210c M7 and X410c M7 (with PCIe Node)	4.3(4a)	6.0(2e)
	UCSC-GPU-H100-80	Cisco UCS C240 M7	4.3(4a)	6.0(2e)
NVIDIA L4:70W, 24GB, 1-slot HHHL GPU	UCSC-GPU-L4	Cisco UCS C240 M8 and C220 M8	4.3(6a)	6.0(2e)
		Cisco UCS C245 M8	4.3(5a)	6.0(2e)
		Cisco UCS C220 M7 and C240 M7	4.3(2b)	6.0(2e)
		Cisco UCS X215c M8 (with PCIe Node)	4.3(5a)	6.0(2e)
NVIDIA P4	UCSC-GPU-P4	Cisco UCS C220 M5	3.2(3a)	6.0(2e)

GPU/GPU PCIe Node	PID	Supported Servers	Minimum Software Version	Suggested Software Version
NVIDIA M10	UCSC-GPU-M10	Cisco UCS C240 M5 and C480 M5	3.2(3a)	6.0(2e)
NVIDIA GRID P6 Front Mezzanine	UCSB-GPU-P6-F	Cisco UCS B200 M5	3.2(1d)	6.0(2e)
		Cisco UCS B480 M5	3.2(2b)	6.0(2e)
NVIDIA GRID P6 Rear Mezzanine	UCSB-GPU-P6-R	Cisco UCS B200 M5	3.2(1d)	6.0(2e)
		Cisco UCS B480 M5	3.2(2b)	6.0(2e)
TESLA A30, PASSIVE, 180W, 24GB	UCSC-GPU-A30-D	Cisco UCS C240 M7	4.3(2b)	6.0(2e)
	UCSC-GPU-A30	Cisco UCS C240 M6	4.2(1d)	6.0(2e)
		Cisco UCS C245 M6	4.2(1i)	6.0(2e)
TESLA A40 RTX, PASSIVE, 300W, 48GB	UCSX-GPU-A40-D	Cisco UCS X210c M7 and X210c M6 (with PCIe Node)	4.3(4a)	6.0(2e)
		Cisco UCS X410c M7 (with PCIe Node)	4.3(4a)	6.0(2e)
	UCSC-GPU-A40-D	Cisco UCS C240 M7	4.3(2b)	6.0(2e)
	UCSC-GPU-A40	Cisco UCS C240 M6	4.2(1d)	6.0(2e)
		Cisco UCS C245 M6	4.2(1i)	6.0(2e)
		Cisco UCS C480 M5	3.2(3a)	6.0(2e)

GPU/GPU PCIe Node	PID	Supported Servers	Minimum Software Version	Suggested Software Version
TESLA A100, PASSIVE, 300W, 80GB12	UCSX-GPU-A100-80-D	Cisco UCS X210c M7 and X210c M6 (with PCIe Node)	4.3(4a)	6.0(2e)
		Cisco UCS X410c M7 (with PCIe Node)	4.3(4a)	6.0(2e)
	UCSC-GPUA100-80-D	Cisco UCS C240 M7	4.3(2b)	6.0(2e)
	UCSC-GPU-A100-80	Cisco UCS C240 M6	4.2(1d)	6.0(2e)
		Cisco UCS C245 M6	4.2(1i)	6.0(2e)
		All Cisco UCS C-Series M5	4.2(2c)	6.0(2e)
TESLA A10, PASSIVE, 150W, 24GB	UCSC-GPU-A10	Cisco UCS C240 M6	4.2(1d)	6.0(2e)
		Cisco UCS C245 M6	4.2(1i)	6.0(2e)
NVIDIA H200-NVL GPU	UCSC-GPU-H200-NVL	Cisco UCS C240 M8	4.3(6c)	6.0(2e)

Deprecated Hardware and Software in Cisco UCS Manager

Release 6.0(2b)

Cisco UCS Manager introduces unified infrastructure firmware management for Cisco UCS 6600 Series and 6500 Series Fabric Interconnects and deprecates support for Service Pack firmware packages; separate Service Pack files and the startup version are no longer utilized. All maintenance fixes, security patches, and updates are now delivered within a single, unified Infrastructure Software Bundle. Lightweight upgrades are not supported in this unified model, requiring all infrastructure upgrades to follow the standard Auto Install process. The standard Auto Install process requires necessary reboots of the Fabric Interconnects to ensure all consolidated fixes are correctly applied.

Release 6.0(1b)

Beginning with Cisco UCS Manager Release 6.0(1b), the following hardware are no longer supported:

- Cisco UCS FI Models:
  - UCS-FI-6300-E6U16
  - UCS-FI-6300-E6-16UP
  - UCS-FI-6332-16UP

- UCS-FI-6332
- UCS-FI-M-6324

- IOM Models:
  - UCS-IOM-2208XP
  - UCS-IOM-2204XP
  - UCS-IOM-2304
  - UCS-IOM-2304V2

- FEX Models:
  - N2K-C2248TP-1GE
  - N2K-C2248T-1GE
  - N2K-C2148T-1GE
  - N2K-C2232PP-10GE
  - N2K-C2232TM-10GE
  - N2K-C2232TM-E-10GE
  - N2K-C2348UPQ-10GE

Capability Catalog

The Cisco UCS Manager Capability Catalog is a set of tunable parameters, strings, and rules. Cisco UCS uses the catalog to update the display and configurability of components such as newly qualified DIMMs and disk drives for servers.

The Capability Catalog is embedded in Cisco UCS Manager, but at times it is also released as a single image file to make updates easier.

The following table lists the PIDs added in this release and maps UCS software releases to the corresponding Capability Catalog file.

Table 22: Version Mapping

UCS Release	Catalog File Name	Additional PIDs in this Release
6.0(2e)	ucs-catalog.6.0.2e.T.bin	—
6.0(2d)	ucs-catalog.6.0.2d.T.bin	GPU: • UCSX-GPU-RTXP4500 UCSC-GPU-RTX6000D

UCS Release	Catalog File Name	Additional PIDs in this Release
6.0(2c)	ucs-catalog.6.0.2c.T.bin	Peripherals: • UCSC-P-N3220L (Crypto disabled) • UCSC-P-N3220 (Crypto disabled) Drives: • UCS-NVE11T9K2V9 • UCS-NVE13T8K2V9 • UCS-NVE17T6K2V9 • UCS-NVE115T3K2V9 • UCS-NVE130T7M4V
6.0(2b)	ucs-catalog.6.0.2b.T.bin	Cisco UCS Fabric Interconnect and Components: • FI: UCS-FI-6652-U • Fan: UCS-FAN-6652 • Accessory and blank: UCS-ACC-6652 Cisco UCS X410c M8 Compute Node: UCSX-410c-M8 Peripherals: • UCSC-P-NC3220 • UCSC-P-NC3220L GPU: • UCSC-GPU-RTXP6000
6.0(1h)	ucs-catalog.6.0.1h.T.bin	—
6.0(1f)	ucs-catalog.6.0.1f.T.bin	—
6.0(1e)	ucs-catalog.6.0.1e.T.bin	—
6.0(1d)	ucs-catalog.6.0.1d.T.bin	—
6.0(1c)	ucs-catalog.6.0.1c.T.bin	—

UCS Release	Catalog File Name	Additional PIDs in this Release
6.0(1b)	ucs-catalog.6.0.1c.T.bin	Cisco UCS Fabric Interconnect and Components: • FI: UCS-FI-6664-U • PSU and fan: UCS-PSU-6600-AC, UCS-FAN-6664 • Accessory and blank: UCS-ACC-6664 Controller: • UCSX-X10C-PTE3

Related Resources

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

- Release Bundle Contents for Cisco UCS Software
- Cisco UCS C-series Rack Server Integration Guides
- Cisco UCS C-series Software Release Notes
- Release Notes for Cisco Intersight Infrastructure Firmware
- Release Notes for Cisco UCS Central
- Cisco UCS Manager Upgrade/Downgrade Support Matrix Tool
- Cisco UCS Equivalency Matrix for Cisco Intersight, Cisco IMC, and Cisco UCS Manager Tool
- Cisco UCS Manager Internal Dependencies Matrix Tool
- Cisco UCS Manager Internal Dependencies, Release 6.0
- Cisco UCS Manager Cross Version Firmware Matrix Tool
- Cisco UCS Manager Cross-Version Firmware Support, Release 6.0

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)

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.

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