Release Notes for Cisco Intersight Managed Mode Server Firmware, Release 4.1(3)

First Published: 2024-01-17

Last Modified: 2024-12-04

Overview

Change in Firmware Version Schema New

- **X-Series M6 Server Firmware Bundle**: Post server firmware release 5.0(4g) number is in a number format instead of a letter format.
- **C-Series M5 and M6 Server Firmware Bundle**: Post server firmware release version number is in a number format instead of a letter format.
- **B-Series M5 and M6 Server Firmware Bundle**: Post server firmware release version number is in the 5.x series and in a number format instead of a lett
- **Infrastructure Firmware Bundle**: With infra firmware release 4.3(2) and lat version number is in a number format instead of a letter format.

For example: 4.3(2.230117), where "23" represents the year and "0117" show incremental build number.

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

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

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

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

Supported Cisco UCS servers managed through Intersight are:

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

  These include Cisco UCS B-Series, C-Series, and X-Series servers connected to Intersight through Cisco UCS Fabric Interconnects.



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

- **Intersight Standalone Mode servers:**

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

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

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

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

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

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

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

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

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

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

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

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

Latest Supported Firmware for End-of-Life Intersight Managed Mode Servers

Platform	Supported Latest Firmware version
Cisco UCS C-Series M5 (C240)	4.3(2.250021)
Cisco UCS C-Series M5 (C220, C480)	4.3(2.250016)
Cisco UCS C-Series M6 (C220, C240)	6.0(1.250127)
Cisco UCS B-Series M5 (B200, B480)	6.0(1.250126)

Platform	Supported Latest Firmware version
Cisco UCS B-Series M6 (B200)	6.0(1.250126)

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

Revision History

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

Revision Date	Description
December 04, 2024	Intersight Infrastructure Firmware version 4.1(3n) has been released. There is no corresponding server firmware in this release.
March 07, 2024	Updated release notes for Cisco UCS C-Series Server Firmware, Release 4.1(3n).
November 27, 2023	Created release notes for Cisco UCS C-Series Server Firmware, Release 4.1(3m). **Note** This release notes include release information starting from 4.1(3m) and continue to cover all subsequent versions. It does not cover any versions prior to 4.1(3m).

New Software Support

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

Cross Version Firmware Support

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

The following table shows the supported Server firmware and Infrastructure firmware versions:

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

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

New Features

New Hardware in Release 4.1(3n) — None

New Hardware in Release 4.1(3m) — None

Security Fixes

Security Fixes in Release 4.1(3n) — None

Security Fixes in Release 4.1(3m)

The following security issues are resolved:

Defect ID - CSCwf30468

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

CVE-2022-40982—Information exposure through microarchitectural state after transient execution in certain vector execution units for some Intel® Processors may allow an authenticated user to potentially enable information disclosure through local access.

CVE-2022-43505—Insufficient control flow management in the BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable denial of service through local access.

Defect ID - CSCwe96259

Cisco UCS C-Series Rack Servers are affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID(s):

CVE-2023-20228—A vulnerability in the web-based management interface of Cisco IMC could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the browser of the targeted user or access sensitive, browser-based information.

Defect ID - CSCwf98321

Cisco UCS S-Series S3260 M4 Rack Servers are affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID(s):

- **CVE-2022-38083**—Improper initialization in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable information disclosure through local access.
- **CVE-2022-43505**—Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable denial of service through local access.

Caveats

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

Open Caveats

Open Caveats for Release 4.1(3n) — None

Open Caveats for Release 4.1(3m)— None

Resolved Caveats

Resolved Caveats for Release 4.1(3n)

The following table lists the resolved caveats in C-Series firmware release 4.1(3n)

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

Resolved Caveats for C-Series Firmware Release 4.1(3m)

The following table lists the resolved caveats for Release 4.1(3m)

Defect ID	Description	First Bundle Affected
CSCwb82433	Cisco UCS C220 M5 servers, equipped with Cisco UCS VIC 1400 series adapter and have Geneve enabled, go offline after the Cisco UCS VIC adapters fail to respond.	4.1(3d)
CSCwe35644	Several ECCs are observed on a single DIMM with no fault from Cisco UCS Manager in Cisco UCS C-Series M5 and M6 servers equipped with 64GB DIMMs (UCS-MR-X64G2RW) and ADDDC enabled.	4.1(3e)

Known Limitations and Behavior

Known Limitations and Behavior for 4.1(3n) — None

Known Limitations and Behavior for 4.1(3m) — None

Related resources

- Release Notes and Release Bundles for Cisco Intersight
- Cisco UCS Equivalency Matrix for Cisco Intersight, Cisco IMC, and Cisco UCS Manager
- Release Notes for Cisco UCS Manager
- Release Notes for Cisco UCS Rack Server Software
- Cisco Baseboard Management Controller Release Notes for Cisco UCS C885A M8 Rack Server
- Cisco UCS Manager and Intersight Release Strategy