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

First Published: 2024-01-17

Last Modified: 2024-03-07

Change in Firmware Version Schema **New**

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

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

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

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

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

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

Overview

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

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

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

IIS manages the following Cisco UCS servers:

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

About the Release Notes

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

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

This document also includes the following:

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

Revision History

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

Revision Date	Description
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).

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

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 Documentation

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