Release Notes for Cisco UCS Manager, Release 3.1

First Published: 2016-01-20

Last Modified: 2020-12-20

Cisco UCS Manager

Cisco UCS™ Manager, release 3.1 provides unified, embedded management of all software and hardware components of the Cisco Unified Computing System™ (Cisco UCS) across multiple chassis, Cisco UCS servers, and thousands of virtual machines. Cisco UCS Manager manages Cisco UCS as a single entity through an intuitive GUI, a command-line interface (CLI), or an XML API for comprehensive access to all Cisco UCS Manager functions. For more information on Cisco UCS Manager, see Cisco UCS Manager on Cisco.com.

This document contains information on new features, resolved caveats, open caveats, and workarounds for Cisco UCS Manager, Release 3.1. This document also includes the following:

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

Support for Web User Interface Post Deprecation of Adobe Flash

The Web user interface of Cisco UCS Manager releases earlier than 3.1(3a) — including the releases on the 2.2 release train — are Java-based and may not be accessible on browser versions that will deprecate support for Adobe Flash on Dec 31, 2020. For more details on the problem description and workarounds, refer to the Field Notice: FN72012.

Revision History

Release	Date	Description
3.1(1e)	January 20, 2016	Created release notes for Cisco UCS Manager, Release 3.1(1e).
	January 22, 2016	Updated Cisco UCS Central integration requirements.
	February 15, 2016	Updated release notes to include support for Cisco UCS 420 M4 on Cisco UCS Mini.
	March 9, 2016	Updated release notes to include support for 3.8TB 2.5 inch Enterprise Value 6G SATA SSD. Added CSCuy46062 to 3.1(1e) Behavior Changes and Known Limitations.
	May 18, 2018	Updated the Resolved Caveats for Release 3.1(1e) with CSCun07367.
	May 28, 2018	Updated the Open Caveats for Release 3.1(1e) with CSCvj59299, CSCvj59301, CSCvj54880, CSCvj54847, CSCvj54187, and their Software Advisory.
3.1(1g)	March 31, 2016	Updated release notes for Cisco UCS Software Release 3.1(1g).
	April 05, 2016	Updated release notes to include support for UCS-IOM-2304 on Cisco UCS Chassis N20-C6508.
	April 18, 2016	Updated release notes for key ring modulus size support. Updated list of power supplies for Cisco UCS FIs.

Release	Date	Description
3.1(1h)	May 20, 2016	Updated release notes for Cisco UCS Software Release 3.1(1h).
	May 24, 2016	Added CSCuz74973 to the Open Caveats for Cisco UCS Software Release 3.1(1e).
	June 14, 2016	Updated the versions for the first bundle affected in the Open Caveats section for Cisco UCS Software Release 3.1(1e).
	June 17, 2016	Corrected a note regarding UCS-ML-1X324RU-G and UCS-ML-1X644RU-G support.
	June 20, 2016	Corrected a note regarding UCS-ML-1X324RV-A and UCS-ML-1X644RV-A support.
	June 21, 2016	Added section for Cisco UCS Mini support.
3.1(1k)	August 29, 2016	Updated release notes for Cisco UCS Software Release 3.1(1k).
3.1(2b)	September 17, 2016	Updated release notes for Cisco UCS Software Release 3.1(2b).
	September 19, 2016	Added CSCvb35827 to the Open Caveats for Cisco UCS Software Release 3.1(2b).
	September 22, 2016	Added CSCvz91263 to the Security Fixes section.
	September 26, 2016	Added CSCvb44879 to the Open Caveats section for Cisco UCS Software Release 3.1(2b).
	September 27, 2016	Updated New Software Features for 3.1(2b) section for VXLAN support.
	October 13, 2016	Added CSCuy13596 to the Resolved Caveats section for Cisco UCS Software Release 3.1(2b).
	May 18, 2018	Updated the Resolved Caveats for Release 3.1(2b) with CSCun07367.
3.1(2c)	October 7, 2016	Updated release notes for Cisco UCS Software Release 3.1(2c).
3.1(2e)	November 23, 2016	Updated release notes for Catalog Release 3.1.2e.T.

Release	Date	Description
3.1(2e)	December 23, 2016	Updated release notes for Cisco UCS Software Release 3.1(2e).
3.1(1l)	January 26, 2017	Updated release notes for Cisco UCS Software Release 3.1(1l).
3.1(2f)	February 28, 2017	Updated release notes for Cisco UCS Software Release 3.1(2f).
3.1(2g)	April 19, 2017	Updated release notes for Cisco UCS Software Release 3.1(2g).
3.1(3a)	April 27, 2017	Updated release notes for Cisco UCS Software Release 3.1(3a).
	May 02, 2017	Removed CSCvd71484 from the Resolved Caveats section for Cisco UCS Software Release 3.1(3a).
	June 25, 2018	Added CSCvf32853 to the Open Caveats section for Cisco UCS Software Release 3.1(3a).
	February 27, 2019	Updated the information for CSCvf32853 in the Open Caveats section for Cisco UCS Software Release 3.1(3a).
3.1(2h)	June 29, 2017	Updated release notes for Cisco UCS Software Release 3.1(2h).
3.1(3b)	June 29, 2017	Updated release notes for Cisco UCS Software Release 3.1(3b).
3.1(3c)	July 24, 2017	Updated release notes for Cisco UCS Software Release 3.1(3c).
3.1(3d)	October 13, 2017	Updated release notes for Cisco UCS Software Release 3.1(3d).
3.1(3e)	November 29, 2017	Updated release notes for Cisco UCS Software Release 3.1(3e).
	December 4, 2017	Updated the **Upgrade and Downgrade Guidelines** section for the minimum supported S3260 release.
3.1(3f)	March 21, 2018	Updated release notes for Cisco UCS Software Release 3.1(3f).

Release	Date	Description
3.1(3h)	May 14, 2018	Updated release notes for Cisco UCS Software Release 3.1(3h).
	July 6, 2018	Updated the Cross-Version Firmware Support to for 2.2(7) and 2.2(8) B and C bundles.
3.1(3j)	July 20, 2018	Updated release notes for Cisco UCS Software Release 3.1(3j).
	August 27, 2018	Added the L1 Terminal Fault caveats — CSCvm02934, CSCvm03356, CSCvm03351, and CSCvm03339 — to the list of Security Fixes.
3.1(3k)	September 11, 2018	Updated release notes for Cisco UCS Software Release 3.1(3k).
	June 3, 2019	Added a known limitation - UCS 6300 Series Fabric Interconnect ASIC Limitation with Passive Cables.
3.1(3l)	January 13, 2020	Updated release notes for Cisco UCS Software Release 3.1(3l).
	December 20, 2020	Added notice: Support for Web User Interface Post Deprecation of Adobe Flash.

Top Reasons to Move to Cisco UCS Manager Release 3.1

Here are the top reasons to move to Cisco UCS Manager Release 3.1:

- Support for new hardware, including UCS 6332 Series Fabric Interconnects, S3260 storage servers, Secure Encrypted Drives, and numerous peripherals.
- Support for HTML5 user interface.
- Support for HTML5 KVM client to facilitate improved management of KVM.
- Cisco UCS Manager Release 3.1(3) is the patch point for the Cisco UCS Manager 3.1 release train.

New Features in Release 3.1

Cisco UCS Manager, Release 3.1 is a unified software release for all supported UCS hardware platforms. The release adds support for HTML5 interface in addition to the Java interface, both of which are available across all platforms.

Note Beginning with Cisco UCS Manager Release 3.1(3a), the Cisco UCS Manager GUI is no longer available as a Java-based application.

New Hardware Features

- New Hardware in Release 3.1(3l) — None
- New Hardware in Release 3.1(3k) — None
- New Hardware in Release 3.1(3j) — None
- New Hardware in Release 3.1(3h) — None
- New Hardware in Release 3.1(3f), on page 7
- New Hardware in Release 3.1(3e) — None
- New Hardware in Release 3.1(3d), on page 8
- New Hardware in Release 3.1(3c) — None
- New Hardware in Release 3.1(3b) — None
- New Hardware in Release 3.1(3a), on page 9
- New Hardware in Release 3.1(2h) — None
- New Hardware in Release 3.1(2g) — None
- New Hardware in Release 3.1(2f) — None
- New Hardware in Release 3.1(2e), on page 9
- New Hardware in Release 3.1(2c) — None
- New Hardware in Release 3.1(2b), on page 10
- New Hardware in Release 3.1(1l) — None
- New Hardware in Release 3.1(1k) — None
- New Hardware in Release 3.1(1h) — None
- New Hardware in Release 3.1(1g), on page 12
- New Hardware in Release 3.1(1e), on page 13

New Software Features

- New Software Features in Release 3.1(3l) — None
- New Software Features in Release 3.1(3k) — None
- New Software Features in Release 3.1(3j) — None
- New Software Features in Release 3.1(3h) — None
- New Software Features in Release 3.1(3f), on page 14
- New Software Features in Release 3.1(3e) — None
- New Software Features in Release 3.1(3d) — None
- New Software Features in Release 3.1(3c)

- New Software Features in Release 3.1(3b) — None
- New Software Features in Release 3.1(3a), on page 15
- New Software Features in Release 3.1(2h) — None
- New Software Features in Release 3.1(2g) — None
- New Software Features in Release 3.1(2f) — None
- New Software Features in Release 3.1(2e) — None
- New Software Features in Release 3.1(2c) — None
- New Software Features in Release 3.1(2b), on page 17
- New Software Features in Release 3.1(1l) — None
- New Software Features in Release 3.1(1k) — None
- New Software Features in Release 3.1(1h) — None
- New Software Features in Release 3.1(1g) — None
- New Software Features in Release 3.1(1e), on page 19

New Hardware in Release 3.1(3f)

Support for the following drives:

- UCS-HD300G10K12G
- UCS-HD600G10K12G
- UCS-HD1T7K12G
- UCS-HD2T7K12G
- UCS-HD12T7KL6GHA
- UCS-HD12T7KL4KHM
- UCS-HD8T7KL4KSM
- UCS-HD10T7KL4KSM
- UCS-HY480GIS3-EP
- UCS-HY19TIS3-EP
- UCS-S3260-HD12T
- UCS-S3260-HD12TR
- UCS-SD400GH3-EP
- UCS-SD800GH3-EP
- UCS-SD16TH3-EP
- UCS-SD32TH3-EP

- UCS-SD38TBIS6-EV
- UCS-SD480GBIS6-EV
- UCS-SD960GBIS6-EV
- UCS-SD480GIS3-EP
- UCS-SD960GIS3-EP
- UCS-SD19TIS3-EP
- UCS-S3260-3SSD4
- UCS-S3260-3SSD8
- UCS-S3260-3SSD16
- UCS-S3260-3SSD32
- UCS-S3260-NVM48
- UCS-S3260-NVM416
- UCS-S3260-NVM432
- UCS-S3260-NVM464

New Hardware in Release 3.1(3d)

- Support for the following drives:
  - UCS-HD8T7KL6GA
  - UCS-HD10T7KL6GA
  - UCS-S3260-G3SD24
  - UCS-S3260-G3SD48
  - UCS-S3260-G3SD160
  - UCS-HY400GSAS3-EP
  - UCS-HY800GSAS3-EP
  - UCS-HY16TSAS3-EP
  - UCS-SD240GBKS4-EB
  - UCS-SD120GBKS4-EB
  - UCS-SD480GBKS4-EB
  - UCS-SD16TBKS4-EB
- Support for the following NVMe drives:
  - UCSC-NVMEM4-H800
  - UCSC-NVMEM4-H1600

- UCSC-NVME-H32003
- UCSC-NVME-H64003
- UCSC-NVME-H76801

New Hardware in Release 3.1(3a)

- Support for Second RAID Controller in the IO Expander on Cisco UCS S3260 (UCS-C3K-M4RAID)
- Support for Dual HBA Controller on Cisco UCS S3260 (UCS-S3260-DHBA)
- Support for the following Qlogic adapters:
  - Support for Qlogic QLE2742 dual-port 32G FC (UCSC-PCIE-QD32GF)
  - Support for Qlogic QLE2562 dual-port 8G FC (N2XX-AQPCI05)
  - Inventory support for Qlogic QLE2672 dual-port 16G FC (UCSC-PCIE-Q2672)

Note Only inventory support, not management support.

- Support for the following Emulex adapters:
  - Support for Emulex LPe32002 dual-port 32G FC (UCSC-PCIE-BD32GF)
  - Support for Emulex LPe32001 single-port 32G (UCSC-PCIE-BS32GF)
  - Support for Emulex LPe16002 dual-port 16G (UCSC-PCIE-E16002)
  - Support for Emulex LPe12002 dual-port 8G (N2XX-AEPCI05)
- Support for Intel X550 dual-port 10GBase-T adapter (UCSC-PCIE-ID10GC)
- Support for the following NVIDIA GPUs:
  - Support for NVIDIA M10 32GB GPU (UCSC-GPU-M10)
  - Support for NVIDIA P100 16GB GPU (UCSC-GPU-P100-16G)
  - Support for NVIDIA P100 12GB GPU (UCSC-GPU-P100-12G)
- Support for AMD Firepro S7150x2 16GB GPU (UCSC-GPU-7150x2)

New Hardware in Release 3.1(2e)

Support for the following CPUs:

- UCS-CPU-E52699AE
- UCS-CPU-E78894E

Support for the following new drives:

- UCS-SD480GBKS-EV

- UCS-SD19TBKSS-EV

New Hardware in Release 3.1(2b)

- Cisco UCS Manager support for the Cisco UCS S3260 system—The Cisco UCS S3260 is a modular, dense storage rack server with dual server nodes, optimized for large data sets used in environments such as big data, cloud, object storage, and content delivery. The Cisco UCS S3260 system is designed to operate in a standalone environment and, starting with Cisco UCS Manager 3.1(2b), as part of the Cisco Unified Computing System with Cisco UCS Manager integration. *Cisco UCS C3260 Server Integration with Cisco UCS Manager, Release 3.1* provides detailed information.
- Cisco UCS B260 and B460 M4 shipping with Intel® Xeon® Processor E7-4800 v4 and E7-8800 v4 series CPUs
- Cisco UCS Mini support introduced for Cisco UCS B260 and B460 M4
- Cisco UCS B420 M4 shipping with Intel® Xeon® Processor E5-4600 v4 series CPUs
- Cisco UCS C460 M4 shipping with Intel® Xeon® Processor E7-8800 v4 series CPUs
- Support for the following CPUs:
  - UCS-CPU-E5-4610E
  - UCS-CPU-E5-4620E
  - UCS-CPU-E5-4627E
  - UCS-CPU-E5-4640E
  - UCS-CPU-E5-4650E
  - UCS-CPU-E5-4655E
  - UCS-CPU-E5-4660E
  - UCS-CPU-E5-4667E
  - UCS-CPU-E5-4669E
  - UCS-CPU-E52650E
  - UCS-CPU-E74809E
  - UCS-CPU-E74820E
  - UCS-CPU-E74830E
  - UCS-CPU-E74850E
  - UCS-CPU-E78860E
  - UCS-CPU-E78867E
  - UCS-CPU-E78870E
  - UCS-CPU-E78880E
  - UCS-CPU-E78890E
  - UCS-CPU-E78891E

    - UCS-CPU-E78893E

- Support for the following Intel® NIC adapters:
    - UCSC-PCIE-IQ10GF
    - UCSC-PCIE-ID10GF
    - UCSC-PCIE-ID40GF

- Support for the following new NVMe-based PCIe storage options:
    - HGST HH-HL PCIe cards for all Cisco UCS M4 rack servers:
        - Cisco UCS (SN150) HH-HL 1900 GB NVMe-based PCIe SSD (UCSC-F-H19001)
        - Cisco UCS (SN150) HH-HL 3800 GB NVMe-based PCIe SSD (UCSC-F-H38001)
    - Intel HH-HL PCIe cards for all Cisco UCS M4 rack servers:
        - Cisco UCS (P3700) HH-HL 800 GB NVMe-based PCIe SSD (UCSC-F-I80010)
        - Cisco UCS (P3700) HH-HL 1600 GB NVMe-based PCIe SSD (UCSC-F-I160010)
        - Cisco UCS (P3600) HH-HL 2000 GB NVMe-based PCIe SSD (UCSC-F-I20003)
    - HGST 2.5” PCIe SSDs for all Cisco UCS M4 rack servers:
        - Cisco UCS (SN100) 2.5” 3800 GB NVMe-based PCIe SSD (UCS-PCI25-38001)
    - Intel 2.5” PCIe SSD for Cisco UCS B200 M4 blade servers and all Cisco UCS M4 rack servers:
        - Cisco UCS (P3700) 2.5” 400 GB NVMe-based PCIe SSD (UCS-PCI25-40010)
        - Cisco UCS (P3600) 2.5” 800 GB NVMe-based PCIe SSD (UCS-PCI25-8003)
        - Cisco UCS (P3700) 2.5” 800 GB NVMe-based PCIe SSD (UCS-PCI25-80010)
        - Cisco UCS (P3600) 2.5” 1600 GB NVMe-based PCIe SSD (UCS-PCI25-16003)

- Support for 4K format disk drives as bootable drives on blade servers with Cisco UCS Manager Release 3.1(2b) and later versions.
- Support for a 10 TB 512e disk drive (UCS-HD10T7KEM). 512e drives are 4K disk drives that can emulate a block size of 512 bytes to maintain compatibility with legacy computing components.
- SAS HBA management support for the following:
    - Cisco UCS SAS 9300-8e 12Gb/s SAS HBA (Pass-through) (UCSC-SAS9300-8e)
    - Cisco 12G Modular SAS HBA (Pass-through) (UCSC-SAS12GHBA) on Cisco UCS C220 M4 and C240 M4 servers
    - Cisco 12G Modular SAS HBA (Pass-through) (UCSC-PSAS12GHBA) on Cisco UCS C220 M4 and C240 M4 servers

- Support for NVIDIA GPU M60 adapter on Cisco UCS C460 M4 servers

- Support for Magma Expander on Cisco UCS C460 M4 servers
- Support for the following SED drives:
  - SFF—2.5” HDD:
    - UCS-HD300G10K9 300GB 12G SAS 10K RPM SFF HDD (SED)
    - UCS-HD600G15K9 600GB 12G SAS 15K RPM SFF HDD (SED)
    - UCS-HD12G10K9 1.2 TB 12G SAS 10K RPM SFF HDD (SED)
    - UCS-HD18G10K9 1.8TB 12G SAS 10K RPM SFF HDD (4K,SED)
  - LFF—3.5” HDD:
    - UCS-HD600G15CK9 600GB 12G SAS 15K PM LFF HDD (SED)
    - UCS-HD4TBK9 4TB SAS 7.2K RPM LFF SED HDD
    - UCS-HD4T12GK9 4TB 12G SAS 7.2K RPM LFF HDD (SED)
    - UCS-HD6T12GAK9 6TB 7.2K RPM LFF HDD (4K, SED)
  - SFF—2.5” SSD:
    - UCS-SD400GBK9 400GB Enterprise Perf 12G SAS SFF SED SSD
    - UCS-SD400GBEK9 400GB Enterprise Perf SAS SFF SSD (10X FWPD, SED)
    - UCS-SD800GBEK9 800GB Enterprise Perf SAS SFF SSD (10X FWPD, SED)
    - UCS-SD16TBEK9 1.6TB Enterprise Perf SAS SFF SSD (10XFWPD, SED)
    - UCS-SD600GBE3K9 600GB Enterprise Perf SATA SFF SSD (3X FWPD, SED)
    - UCS-SD120GBE1K9 120GB Ent Value SFF SSD (SATA) (1X FWPD, SED)
    - UCS-SD480GBE1K9 480GB Enterprise Value SATA SFF SSD (1XFWPD, SED)
    - UCS-SD960GBE1K9 960GB Enterprise Value SATA SFF SSD (1X FWPD, SED)
  - LFF—3.5” SSD:
    - UCS-SD400GBCK9 400GB Enterprise Perf SAS LFF SSD (10X FWPD, SED)
    - UCS-SD800GBCK9 800GB Enterprise Perf SAS LFF SSD (10X FWPD, SED)
- Cisco UCS 6300 switches
- Cisco UCS M-Series servers are no longer supported with Cisco UCS Manager Release 3.1(2b) and later releases.

New Hardware in Release 3.1(1g)

- Cisco UCS B200 M4, C220 and C240 servers shipping with Intel® Xeon® Processor E5-2600 v4 series CPUs.
- Support for Emulex adapter (UCSC-PCIE-E14102B).

- Support for the following CPUs for Cisco UCS B200 M4, C220 M4, and C240 M4 servers:
  - UCS-CPU-E52699E
  - UCS-CPU-E52698E
  - UCS-CPU-E52697AE
  - UCS-CPU-E52697E
  - UCS-CPU-E52695E
  - UCS-CPU-E52690E
  - UCS-CPU-E52683E
  - UCS-CPU-E52680E
  - UCS-CPU-E52667E
  - UCS-CPU-E52660E
  - UCS-CPU-E52658E
  - UCS-CPU-E52650E
  - UCS-CPU-E52650LE
  - UCS-CPU-E52640E
  - UCS-CPU-E52637E
  - UCS-CPU-E52630E
  - UCS-CPU-E52630LE
  - UCS-CPU-E52623E
  - UCS-CPU-E52637E
  - UCS-CPU-E52620E
  - UCS-CPU-E52609E

Please see the software advisory for this release.

New Hardware in Release 3.1(1e)

3rd Generation Fabric Interconnects

- Support for 3rd Generation Fabric Interconnects (UCS 6332 FI, UCS 6332–16UP FI) and UCS IOM 2304
- Support for Cisco Nexus 2348UPQ FEX
- Support for 3rd Generation Cisco VIC 1385 in Cisco UCS Manager
- Support for 3rd Generation VIC 1387 (40G PCIe/mLOM VIC Adapter)

Servers, Cartridge and Peripherals

- Support for CSB-MEZ-INT8955 on B200-M4
- Support for UCSB-GPU-M6 (Tesla) on B200-M4

Note Certain NVIDIA Graphics Processing Units (GPU) do not support Error Correcting Code (ECC) and vGPU together. Cisco recommends that you refer to the release notes published by NVIDIA for the respective GPU to know whether it supports ECC and vGPU together.

- Support fo PCIe SSD on B200 M4
- Support for LSI 9286CV-8e RAID Controller (UCS-RAID9286CV-8E)
- Support for M-Series Broadwell DE/LGA Compute Cartridges
- Support for UCS Mini Secondary Chassis
- Support for QLogic QLE8442 10Gb Dual port 10GBaseT network adapter
- Support for QLogic QLE8442 10Gb Dual port SFP+ network adapter
- Support for NVIDIA GPU M60 adapter on Cisco UCS C240 M4 servers

Note Certain NVIDIA Graphics Processing Units (GPU) do not support Error Correcting Code (ECC) and vGPU together. Cisco recommends that you refer to the release notes published by NVIDIA for the respective GPU to know whether it supports ECC and vGPU together.

- Support for additional Fusion IO adapters
- Support for Cisco UCS C240 NEBS Rack Server
- Support for VIC 1385 network adapter
- Support for VIC 1387 network adapter
- Support for 3.8TB 2.5 inch Enterprise Value 6G SATA SSD (UCS-SD38TBKS4-EV)

New Software Features in Release 3.1(3f)

Feature Enhancements

- TPM 2.0 Firmware Update Capability—A new platform BIOS in the UCS Manager 3.1(3f) patch release fixes the security vulnerability with TPM 2.0 (CVE-2017-15361) for Cisco Unified Computing M4 and M5 servers.

New Software Features in Release 3.1(3c)

Feature Enhancements

- Cisco HyperFlex Support for SED Security Policies and KMIP—Self-Encrypting Drives (SEDs) have a special hardware that encrypts incoming data and decrypts outgoing data in real-time. A media encryption

key controls this encryption and decryption. SEDs need to be locked by providing a security key identifier and a security key. The security key is used to encrypt the media encryption key. You can configure security keys locally, or remotely using a KMIP server. In this release, Cisco HyperFlex HX-Series servers support SED security policies and KMIP. The SED security policies and KMIP configuration must be performed only through the Cisco HyperFlex HX Connect user interface.

New Software Features in Release 3.1(3a)

Scale Improvements

- The number of active VLANs per Cisco UCS domain was increased to 3000 for Cisco UCS 6332 fabric interconnects.
- The number of appliance ports per fabric interconnect was increased to 16 for Cisco UCS 6200 and UCS 6332 fabric interconnects.
- The number of primary VLANs supported in a PVLAN domain was increased from 50 to 150 for Cisco UCS 6200 Series fabric interconnects. The ratio of secondary VLANs to primary VLANs was increased from 30:1 to 200:1 for Cisco UCS 6200 Series fabric interconnects.

Feature Enhancements

- Integrated Server Diagnostics—The Cisco UCS Manager diagnostics tool enables you to verify the health of the hardware components on your servers. It also provides a variety of tests to exercise and stress the various hardware subsystems on the servers, such as memory and CPU.
- Light Weight Upgrades—Cisco UCS Manager Release 3.1(3) introduces light weight upgrades, which delivers security updates for infrastructure and server components through a common service pack bundle. In some cases, UCS Manager service packs may be applied to the UCS fabric interconnects (infrastructure A bundle) without involving a UCS fabric interconnect reboot.
- S3260 Rebranding—Beginning with Cisco UCS Manager Release 3.1(3), Cisco UCS C3260/C3X60 is renamed to Cisco UCS S3260. You may still see certain components in the system labeled as C3260/C3X60. For this release, the terms S3260 and C3260/C3X60 are used interchangeably. Both, S3260 and C3260/C3X60, refer to the same hardware component.
- Server SIOC Connectivity functionality—A Cisco UCS S3260 system now supports Server SIOC Connectivity functionality. Using this functionality, you can configure the data path through both the primary and auxiliary SIOCs when the chassis has a single server and dual-SIOC setup.
- Second RAID Controller and Dual HBA Controller—Cisco UCS S3260 systems support the following:
  - Second RAID controller in the optional I/O expander module
  - Dual HBA Controller

  In a Cisco UCS S3260 system, both servers should have either dual RAID controllers or dual HBA controllers. Different controller types in servers are not supported.
- SED Security Policies and KMIP Support—Self-Encrypting Drives (SEDs) have a special hardware that encrypts incoming data and decrypts outgoing data in real-time. A media encryption key controls this encryption and decryption. SEDs need to be locked by providing a security key identifier and a security key. The security key is used to encrypt the media encryption key. You can configure security keys locally, or remotely using a KMIP server. In this release, Cisco UCS Manager supports SEDs on Cisco UCS C-Series and S-Series servers.

- Smart SSD—Cisco UCS Manager Release 3.1(3) introduces support for monitoring SSD health. This feature provides statistical information about various SSD properties. For each property, a minimum, maximum, and average value is recorded and displayed. This feature also allows you to provide a threshold limit for each property.
- Automatic Configuration of FI-Server Ports—Starting with Cisco UCS Manager Release 3.1(3a), you can use a policy and configure the Fabric Interconnect to automatically change unconfigured ports to server ports when a UCS server is directly attached to the Fabric Interconnect.
- Fabric Evacuation with Auto Install—Starting with Cisco UCS Manager Release 3.1(3), you can use fabric evacuation during Auto Install. If you use fabric evacuation with Auto Install, and fabric evacuation was enabled on the fabric interconnect before Auto Install, fabric evacuation is disabled after Auto Install is complete.
- Custom User Label—Service Profiles now have a custom label field that is visible to the operating system or hypervisor running on the server through the SMBIOS asset tag field.
- HTML5 KVM User Interface Support—Cisco UCS Manager Release 3.1(3) introduces the redesigned HTML5 user interface to facilitate improved management of KVM. HTML5 KVM is only for M3 servers and onwards running Cisco UCS Manager Release 3.1(3). M3 rack servers support HTML5 KVM in Cisco UCS Manager-managed mode only. The minimum Web browser version required for HTML5 KVM is Chrome 45, Firefox 45, IE 11, Opera 35, and Safari 9. For best results, use the latest browser version.
- Power Transaction Enhancement—The Power Transaction Log was added which logs the last five server power transitions, the power transition source timestamp of the latest power transition, and the count of the last consecutive server power transitions from the same source.
- VXLAN Offload—VXLAN with Receive Side-Scaling (RSS) stateless offload is supported on VIC adapters 1340, 1380, 1385, 1387, and SIOC on Cisco UCS C3260 for RHEL 7.0, CENTOS 7.0, SLES 12 SP2 and later releases. VXLAN offload is not supported for IPv6.
- Board Aggregation Role—The Board Aggregation Role is a new feature added to identify the master and slave slots. This only applies to Cisco UCS B460 M4 blade servers.
- Hardware Change Discovery Policy—This policy configures Cisco UCS Manager behavior when a hardware component changes. When Cisco UCS Manager detects any change in the server hardware component, a critical “hardware inventory mismatch” fault is raised. You must acknowledge the server to clear the fault and complete the hardware inventory. After you have acknowledged the server, deep discovery and deep association is triggered.
- Cisco HyperFlex Systems Extended Support—This release supports further integration of Cisco HyperFlex Systems with Cisco UCS Manager through improved setup capabilities for HyperFlex Systems with Cisco UCS. HyperFlex Systems add support for the following Cisco UCS Manager features:
  - Automatic Configuration of FI-Server Ports—Enables you to automatically configure the fabric interconnect server ports.
  - SED Security Policies—Enables you to configure local security keys for Self-Encrypting Drives (SEDs).
- Cisco UCS Manager Database Health Monitoring—Cisco UCS Manager provides proactive health check and recovery mechanisms to improve the integrity of the Cisco UCS Manager database. These mechanisms enable active monitoring of the database health.

- Graphics Card Policies—You can now create a graphics card policy and configure the various modes for the graphics card.
- VLAN Groups in vNIC Templates—You can select VLAN groups in addition to any individual VLAN, while creating a vNIC template.
- Virtual Volume Support—Virtual volume support is now supported for ESXi 5.5 and higher.
- Disk Group Policy Enhancement—With this disk group policy enhancement, you can now include JBOD drives in a disk group policy to create LUNs.

New Software Features in Release 3.1(2b)

- Chassis Profile and Chassis Firmware Pack—Cisco UCS Manager now supports chassis profiles and chassis firmware packs to update the chassis components in Cisco UCS S3260 systems.
- Disk Zoning—You can assign chassis level storage disk drives to the server nodes in a Cisco UCS S3260 system by using disk zoning policy.
- Factory Reset of Servers—Cisco UCS Manager enables you to reset a server to its factory settings. By default, the factory reset operation affects only the BIOS and not the storage drives and FlexFlash drives. This is to prevent any loss of data. However, you can choose to reset these devices to a known state as well.
- Chassis Management Controller (CMC) Secure Boot—Cisco UCS Manager enables support of CMC secure boot for Cisco UCS S3260 systems. When CMC secure boot is enabled, only Cisco-signed firmware images can be installed and run on the CMC.
- vNIC Redundancy Pair—Supports two vNICs/vHBAs that are being configured with a common set of parameters through the vNIC/vHBA template pair. This prevents the configuration between two vNICs/vHBAs from going out of sync. Multiple vNIC/vHBA pairs can be created from the same vNIC/vHBA template pair.
- VXLAN with Receive Side-Scaling (RSS) Support for ESX 6.x—Cisco UCS Manager Release 3.1(2b) now supports VXLAN with RSS stateless offload on VIC adapters 1340, 1380, 1385, 1387, and the SIOCs on Cisco UCS S3260 for ESXi 6.0 and later releases. VXLAN offload is not supported for IPv6.
- Consistent Device Naming (CDN) support for Red Hat Enterprise Linux—CDN support has been expanded to include Red Hat Enterprise Linux 6.X and Red Hat Enterprise Linux 7.X.
- Host Firmware Package Enhancement—Local disk firmware is excluded from the host firmware package by default.
- SAS Expander Support—Cisco UCS Manager Release 3.1(2b) and later releases support direct firmware upgrade and downgrade on SAS expanders for Cisco UCS C240, C220, and C460 M4 servers.
- B-Series and C-Series Server Firmware Bundle Enhancement – In releases earlier than Cisco UCS Manager Release 3.1(2b), firmware for endpoints that were common to both the B-Series and C-Series server software bundles was available only in the B-Series server software bundle. Starting with Cisco UCS Manager Release 3.1(2b), the firmware for these common endpoints is available in both the B-Series and C-Series server software bundles. With this enhancement, customers using only C-series servers need not download the B-Series server firmware bundle anymore.

Note Selecting only one of B-Series or C-Series package versions while using auto-install may impact the endpoints that are common to both blade and rack mount servers. To selectively update only blade or rack mount servers, select the appropriate firmware packages and review the impacted endpoints to ensure that there are no unexpected firmware changes or server reboots.

- Power Management Enhancements—Cisco UCS Manager Release 3.1(2b) introduces the following enhancements:
  - Power management support for Cisco UCS C220 M4 and C240 M4 rack servers.
  - Power group support for Fabric Interconnects and Fabric Extenders.
- Cisco usNIC—Libfabric support for Cisco usNIC in Open MPI. To benefit from Cisco usNIC, your applications must use the Message Passing Interface(MPI), or Libfabric interface instead of sockets or other communication APIs.
- FC Zones Enhancement—Support for creating and deleting user-defined FC zones and FC zone profiles.
- Ability to perform Cisco UCS Manager initial configuration without console connectivity based on DHCP lease availability.
- Multicast Hardware Hash—In a port channel, by default, ingress multicast traffic on any port in the fabric interconnect selects a particular link between the IOM and the fabric interconnect to egress the traffic. To reduce potential issues with the bandwidth, and to provide effective load balancing of the ingress multicast traffic, hardware hashing is used for multicast traffic. When multicast hardware hashing is enabled, all links between the IOM and the fabric interconnect in a port channel can be used for multicast traffic.
- Preserving the following properties during backup or import operations:
  - User-defined labels for Chassis, FEX, Rack Servers, IOMs and Blade Servers
  - Assigned IDs for Chassis, FEX and Rack Servers
- NVMe PCIe SSD Inventory—Cisco UCS Manager discovers, identifies, and displays the inventory of Non-Volatile Memory Express (NVMe) Peripheral Component Interconnect Express (PCIe) SSD storage devices. You can view the health of the storage devices in the server. NVMe with PCIe SSD storage devices reduce latency, increase input/output operations per second (IOPS), and lower power consumption compared to SAS or SATA SSDs.

Note Hot insertion and removal of NVMe SSD are not supported.

NVMe boot is not supported from Cisco UCS Manager.

- Support for 160 LDAP Group Maps—Cisco UCS Manager now supports a maximum of 160 LDAP group maps.
- Power Synchronization between Servers and Their Associated Service Profiles —Cisco UCS Manager includes a global (default) power sync policy to synchronize the power state between the associated

service profiles and the servers when the desired power state of the service profile differs from the actual power state of the server.

- Graceful Shutdown—When you acknowledge a server reboot using the graceful shut down options or a change in the service profile that requires the server reboot, Cisco UCS Manager waits until the time specified time in the maintenance policy before performing a hard shut down.
- HA Version Holder Replacement—You can now specify preferred HA version holders. When you trigger a reelection of version holders, these new preferred HA devices are selected first.

Note HA version holder replacement is not supported on Cisco UCS Mini.

- FNIC tunables now has two new options that are available for fibre channel adapter policies for Windows environments.
  - **IO Retry Timeout**—This option adjusts the IO retry timeout after a pending command expires on a network device.
  - **LUN Queue Depth**—This setting adjusts the initial queue depth for all LUNs on the adapter.
- HTML 5 Interface User Interface Improvements—Introduced the redesigned Cisco UCS Manager HTML 5 user interface to facilitate improved management of the Cisco UCS Manager ecosystem.
- Out of Band Disk Inventory for SAS HBA—Cisco UCS now supports out-of-band inventory of disks connected to a SAS HBA 12G storage controller.
- Drive Sled Based PID Determination—A drive sled, which is provided with a disk drive, is the electrical and mechanical contact of the disk with the slot. A PID is assigned to this combination of disk drive and sled. Disk slots for rack servers are different from the disk slots for Cisco UCS S3260 systems. Therefore, the same disk will have different drive sleds for rack servers and Cisco UCS S3260 systems, and, during inventory, will display different PIDs based on the server where it is found.
- Cisco UCS Manager 3.1(2) introduces the capability to detect and alert users to issues relating to 40Gb link quality.
- 

Attention Starting with Cisco UCS Manager Release 3.1(2b), Cisco UCS Manager no longer supports management of Cisco UCS M-Series servers.

New Software Features in Release 3.1(1e)

Unified release for all UCS platforms

- Cisco UCS 6332 and 6332-16UP fabric interconnect with B-Series and C-Series Servers

Software Enablement for New Hardware (Listed in the New hardware section)

Scale improvements

- 128 LDAP group support

- Cisco UCS Mini network scale improvements including support for a second UCS Chassis in a UCS Mini deployment

Feature Enhancements

- HTML5 user interface support for UCS 6332, UCS 6332 16UP, UCS 6248UP and UCS 6296UP and UCS 6324 fabric interconnects. This includes search option that enables you to search for entities in the system from this location. Using this search option, you can perform Create, List and View actions.
- The option to exclude components has been added to Host Firmware Packages.
- Maintenance Policy provides a **On Next Boot** option
- Firmware upgrade checks the VIF/interface status after the fabric interconnect upgrade
- Locator LED support for server hard-disks
- Provision to reset peer IOM modules to factory defaults
- Provision to suppress VIF down alert (code: F0283) when server OS is shutdown or server is powered off
- Prevent firmware upgrade if unsupported or deprecated hardware components are in the Cisco UCS hardware configuration
- Enhanced Health Monitoring includes low kernel memory and parity errors
- Enhanced Power Capping across all platforms includes power supply redundancy method for 220 V (Watts) and 110 V (Watts), power management during Power ON operations
- WellsBurg PCH support in Cisco UCS Manager
- vnic template CDN feature enhancement
- Cisco SSL FOM 4.1 version support (replacing open SSL)
- Common criteria compliance and FIPS compliance certification
- CSDL vulnerability and PSIRT fixes
- SHA-2 certificate support has been added

Deprecated Hardware, Software, and Third Party Adapters Support in Cisco UCS Manager

Deprecated Hardware

Starting with Cisco UCS Manager Release 3.1(3a), Cisco UCS Manager does not support the hardware listed in the following table:

Table 1: Deprecated hardware from Release 3.1(3a)

Hardware Type	Product
Adapters - Blade Servers	UCSB-MEZ-ELX-03
	UCSB-MEZ-QLG-03
	N20-AE0102
	N20-AQ0102
Blade Servers	B250 M2 (N20-B6625-2)

Starting with Cisco UCS Manager Release 3.1(2b), Cisco UCS Manager does not support the hardware listed in the following table:

Table 2: Deprecated hardware from Release 3.1(2b)

Hardware Type	Product
Chassis	UCSME-4308 modular chassis
Cartridges	UCSME-M142
	UCSME-1414
	UCSME-2814

Starting with Cisco UCS Manager Release 3.1(1e), Cisco UCS Manager does not support the hardware listed in the following table:

Table 3: Deprecated hardware from Release 3.1(1e)

Hardware Type	Product
Fabric Interconnects	UCS 6120 (N10-S6100) UCS 6140 (N10-S6200)
IO Modules	2104 FEX (N20-I6584)
Blade Servers	B200 M1 (N20-B6620-1) B250 M1 (N20-B6620-2) B230 M1 (N20-B6730-1) B440 M1 (N20-B6740-2)
Adapters	E M71KR-E (N20-AE0002) Q M71KR-Q (N20-AQ0002) Intel 82598KR (N20-AI0002) M81KR (N20-AC0002) Broadcom M51KR-B BCM 57711 Mezz (N20-AB0002)

Hardware Type	Product
Rack Mount Servers	C210 M2 (R210-2121605W) C460 M2 (UCSC-BASE-M2-C460) C200 M2 (UCSC-BSE-SFF-C200) C250 M2 (R250-2480805W) C260 M2 (C260-BASE-2646) C420 M3
Adapters - Rack Servers	N2XX-ACPCI01 Cisco UCS CNA M61KR-I Intel (N20-AI0102) Broadcom 57711 Dual Port (N2XX-ABPCI02) Cisco UCS P81E VIC (N2XX-ACPCI01) Emulex OneConnect OCe10102-F (N2XX-AEPCI01) Qlogic QLE 8152-CNA (N2XX-AQPCI01)

Important Before you upgrade to Cisco UCS Manager, Release 3.1, you must decommission and remove all deprecated hardware from your system. If you have any deprecated hardware in your system, the infrastructure upgrade fails and rolls back to earlier release.

Make sure to follow recommended upgrade guidelines in the Cisco UCS Manager Firmware Management Guide, Release 3.1, from Cisco UCS Manager Configuration Guides.

Deprecated Software

Cisco UCS Manager Java GUI—Beginning with Cisco UCS Manager Release 3.1(3a), the Cisco UCS Manager GUI is no longer available as a Java-based application.

VM-FEX— Release 3.1(1e) does not support ESXi configuration on VM FEX. However, support has been added from Release 3.1(1g).

Deprecated Third Party Adapters

Table 4: Third party adapter support for Cisco UCS FI 6200, 6332, 6332-16UP, and 6324 series

Adapter	Release	Support for Cisco UCS FI 6200 Series	Support for Cisco UCS FI 6332, 6332-16UP, and Cisco UCS 6324
UCSC-PCIE-ID10GF	3.1(2b)	Yes	Yes
UCSC-PCIE-ID40GF	3.1(2b)	—	Yes
UCSC-PCIE-IQ10GF	3.1(2b)	—	—
UCSB-MEZ-QLG-03	3.1(1g)	Yes	—

Adapter	Release	Support for Cisco UCS FI 6200 Series	Support for Cisco UCS FI 6332, 6332-16UP, and Cisco UCS 6324
UCSB-MEZ-ELX-03	3.1(1g)	Yes	—
N20-AQ0102	3.1(1g)	Yes	—
N20-AE0102	3.1(1g)	Yes	—

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 and some previous C-Series standalone releases. For example, Cisco UCS Manager Release 3.1(1) is integrated with C-Series Standalone Release 2.0(10) for C220 and C240 M4 servers, and Release 2.0(9) for all other M3 and M4 servers. Hence, it supports all the M4 and M3 servers supported by C-Series Standalone releases. The Internal Dependencies, on page 29 section provides a detailed list of servers supported by Cisco UCS Manager.

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

Table 5: Cisco UCS Manager and C-Series Software releases for C-Series Servers

Cisco UCS Manager Release	C-Series Standalone Release Included	C-Series Servers Supported by the C-Series Standalone Releases
3.1(3f) - 3.1(3l)	3.0(4)	All M3/M4[1]
3.1(3a) - 3.1(3e)	3.0(3)	All M3/M4[2]
3.1(2)	2.0(13)	All M3/M4
3.1(1)	2.0(10)	C220 M4, C240 M4 only
	2.0(9)	All other M3/M4
2.2(8)	2.0(12)	C460 M4 only
	2.0(10)	C220 M4, C240 M4 only
	1.5(9)	C420-M3, C260-M2, C460-M2 only
	2.0(9)	For all other M3/M4
2.2(7)	2.0(10)	C220 M4, C420 M4 only
	1.5(8)	C420 M3, C260 M2, C460 M2 only
	2.0(8)	For all other M3/M4

Cisco UCS Manager Release	C-Series Standalone Release Included	C-Series Servers Supported by the C-Series Standalone Releases
2.2(6)	1.5(8)	C420 M3, C260 M2, C460 M2 only
	2.0(8)	For all other M3/M4
2.2(5)	1.5(7)	C420 M3, C260 M2, C460 M2 only
	2.0(6)	For all other M3/M4
2.2(4)	1.5(7)	C420 M3, C260 M2, C460 M2 only
	2.0(4)	For all other M3/M4
2.2(3)	1.5(7)	C420 M3, C260 M2, C460 M2 only
	2.0(3)	For all other M3/M4

[1] Except for C420 M3(deprecated)
[2] Except for C420 M3(deprecated)

Cisco UCS Mini Support

The following feature introduced in Cisco UCS Manager, Release 3.1(2b) is not supported on Cisco UCS Mini:

- HA Version Holder Replacement

The following features for Cisco UCS Mini are not supported in Cisco UCS Manager, Release 3.1(1e) and later releases:

- Traffic Monitoring Session for SAN
- MAC Security
- Private VLAN
- VXLAN
- NVGRE
- usNIC
- VLAN Compression

System Requirements

Cisco UCS Manager and KVM Launch Manager GUI are available only as HTML5-based applications. You can launch the KVM console from the Cisco UCS Manager GUI or KVM Launch Manager GUI as a Java application or an HTML5-based application.

The Java-based KVM client requires Java Runtime Environment (JRE) 1.7.x or higher.

Important Beginning with Cisco UCS Manager Release 3.1(3a), the Cisco UCS Manager GUI is no longer available as a Java-based application.

Cisco UCS Central Integration

Cisco UCS Manager Release 3.1 can only be registered with Cisco UCS Central, Release 1. 4 or higher.

Supported Operating Systems

Operating System	Minimum Required Memory
Microsoft Windows 7 or higher	8.0 GB
Red Hat Enterprise Linux 5.10 or higher for M3 servers Red Hat Enterprise Linux 6.4 or higher for M4 servers	8.0 GB
Mac OS X 10.9 or higher	8.0 GB

Supported Web Browsers

Cisco UCS Manager GUI	Web Browsers
HTML5	Microsoft Internet Explorer 11 or higher Mozilla Firefox 45 or higher Google Chrome 45 or higher Apple Safari version 9 or higher Opera version 35 or higher

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).

The following table lists the mixed A, B, and C bundle versions that are supported on Cisco UCS 6200 and 6300 fabric interconnects:

Table 6: Mixed Cisco UCS Releases Supported on Cisco UCS 6200 and 6300 Fabric Interconnects

	Infrastructure Versions (A Bundles)										
Host FW Versions (B or C Bundles)	2.2(1)	2.2(2)	2.2(3)	2.2(4)	2.2(5)	2.2(6)	2.2(7)	2.2(8)	3.1(1)	3.1(2)	3.1(3)
2.2(1)	6200	6200	6200	6200	6200	6200	6200	6200	6200	6200	6200
2.2(2)	—	6200	6200	6200	6200	6200	6200	6200	6200	6200	6200
2.2(3)	—	—	6200	6200	6200	6200	6200	6200	6200	6200	6200
2.2(4)	—	—	—	6200	6200	6200	6200	6200	6200	6200	6200
2.2(5)	—		—	6200	6200	6200	6200	6200	6200	6200	6200
2.2(6)	—	—	—	6200[1]	6200[1]	6200	6200	6200	6200	6200	6200
2.2(7)	—	—	—	6200[1]	6200[1]	6200[1]	6200	6200	6200	6200	6200
2.2(8)	—	—	—	6200[1]	6200[1]	6200[1]	6200	6200	6200	6200	6200
3.1(1)	—	—	—	—	—	—	—	—	6200,6332, 6332-16UP	6200,6332, 6332-16UP	6200,6332, 6332-16UP
3.1(2)	—	—	—	—	—	—	—	—	6200,6332, 6332-16UP	6200,6332, 6332-16UP	6200,6332, 6332-16UP
3.1(3)	—	—	—	—	—	—	—	—	6200,6332, 6332-16UP	6200,6332, 6332-16UP	6200,6332, 6332-16UP

[3] Beginning with Cisco UCS Manager Release 2.2(4), and for M4 servers, a lower version of the infrastructure A bundle will be compatible with the previous version and higher version of B and C server bundles. For example, the Cisco UCS Manager Release 2.2(4)A bundle will be supported with any of the following B bundles for B200-M4 servers: 2.1(1)B, 2.1(2)B, 2.1(3)B, 2.2(1)B, 2.2(2)B, 2.2(3)B, 2.2(4)B, 2.2(5)B, 2.2(6)B, 2.2(7)B.

Note For M1, M2, M3 servers, only N, N-1 cross-version firmware is supported. For example, for B200 M3 servers, the 2.2(4)A bundle will be supported with 2.1(1)B, 2.1(2)B, 2.1(3)B, 2.2(1)B, 2.2(2)B, 2.2(3)B, and 2.2(4)B bundles).

The following table lists the mixed A, B, and C bundle versions that are supported on Cisco UCS Mini fabric interconnects:

Table 7: Mixed Cisco UCS Releases Supported on Cisco UCS Mini Fabric Interconnects

	Infrastructure Versions (A Bundles)				
Host FW Versions (B or C Bundles)	3.0(1)	3.0(2)	3.1(1)	3.1(2)	3.1(3)
3.0(1)	6324	6324	6324	6324	6324
3.0(2)	—	6324	6324	6324	6324
3.1(1)	—	—	6324	6324	6324
3.1(2)	—	—	6324	6324	6324
3.1(3)	—	—	6324	6324	6324

The following table lists the mixed B, C bundles that are supported on all platforms with 3.1 bundle:

Table 8: Mixed B, C, M Bundles Supported on All Platforms with the 3.1(1)A Bundle

	Infrastructure Versions (A Bundles)		
Host FW Versions (B, C, or M Bundles)	3.1(1)		
	6200	6300	6324
	ucs-k9-bundle-infra.3.1.x.xxx.A.bin	ucs-6300-k9-bundle-infra.3.1.x.xxx.A.bin	ucs-mini-k9-bundle-infra.3.1.x.xxx.A.bin
2.2(1), 2.2(2), 2.2(3), 2.2(4), 2.2(5), 2.2(6) (B, C Bundles)	Yes	—	—
2.2(7), 2.2(8) (B, C Bundles)	Yes	—	—
2.5(1), 2.5(2) (M Bundle)	Yes	—	—
3.0(1), 3.0(2) (B, C Bundles)	—	—	Yes
3.1(1), 3.1(2), 3.1(3) (B, C Bundles)	Yes	Yes	Yes
3.1(1) (M Bundle)	Yes	—	—

Table 9: Mixed B, C Bundles Supported on All Platforms with the 3.1(2)A Bundle

	Infrastructure Versions (A Bundles)		
Host FW Versions (B, C Bundles)	3.1(2)		
	6200	6300	6324
	ucs-k9-bundle-infra.3.1.x.xxx.A.bin	ucs-6300-k9-bundle-infra.3.1.x.xxx.A.bin	ucs-mini-k9-bundle-infra.3.1.x.xxx.A.bin
2.2(1), 2.2(2), 2.2(3), 2.2(4), 2.2(5), 2.2(6) (B, C Bundles)	Yes	—	—
2.2(7), 2.2(8) (B, C Bundles)	Yes	—	—
3.0(1), 3.0(2) (B, C Bundles)	—	—	Yes
3.1(1), 3.1(2), 3.1(3) (B, C Bundles)	Yes	Yes	Yes

Table 10: Mixed B, C Bundles Supported on All Platforms with the 3.1(3)A Bundle

	Infrastructure Versions (A Bundles)		
Host FW Versions (B, C Bundles)	3.1(3)		
	6200	6300	6324
	ucs-k9-bundle-infra.3.1.x.xxx.A.bin	ucs-6300-k9-bundle-infra.3.1.x.xxx.A.bin	ucs-mini-k9-bundle-infra.3.1.x.xxx.A.bin
2.2(1), 2.2(2), 2.2(3), 2.2(4), 2.2(5), 2.2(6) (B, C Bundles)	Yes	—	—
2.2(7), 2.2(8) (B, C Bundles)	Yes	—	—
3.0(1), 3.0(2) (B, C Bundles)	—	—	Yes
3.1(1), 3.1(2), 3.1(3) (B, C Bundles)	Yes	Yes	Yes

Important If you implement cross-version firmware, you must ensure that the configurations for the Cisco UCS domain are supported by the firmware version on the server endpoints.

Minimum Bundle Version Requirements for Cisco UCS Manager Features

The following Cisco UCS Manager 3.1 features require the specified minimum B,C bundle version to perform expected operations:

Table 11: Minimum Bundle Version Requirements for Cisco UCS Manager Features

Feature	Bundle version
Maintenance Policy provides a **On Next Boot** option	3.1(1e)
Enhanced Health Monitoring includes low kernel memory and parity errors	3.1(1e)
Enhanced Power Capping across all platforms includes power supply redundancy method for 220 V (Watts) and 110 V (Watts), power management during Power ON operations	3.1(1e)
Locator LED support for server hard-disks	3.1(1e)

Internal Dependencies

The following sections provide information on the interdependencies between Cisco UCS hardware and versions of Cisco UCS Manager.

- 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.

6200 Series and 6332 Fabric Interconnects and Components

Blade Servers

Note In a mixed firmware configuration, we recommend that the minimum server bundle corresponds to the Minimum Software Version. The infrastructure must be at or above the Minimum Software Version.

Table 12: Minimum Host Firmware Versions for Blade Servers

Servers	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP FI	Minimum Software Version UCS 6332, 6332-16UPFI	Recommended Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI
	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2304	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2304
B22 M3 E5-2400 B22 M3 E5-2400 v2	2.2(1b) 2.2(2e)	3.1(1e) 3.1(1e)	3.1(1e)	3.1(3l)
B200 M2	2.2(2e)	3.1(1e)	3.1(1e)	3.1(3l)
B200 M3 E5-2600 B200 M3 E5-2600 v2	2.2(1b) 2.2(2e)	3.1(1e) 3.1(1e)	3.1(1e)	3.1(3l)
B200 M4	2.2(3a)	3.1(1e)	3.1(1e)	3.1(3l)
B230 M2	2.2(1b)	3.1(1e)	3.1(1e)	3.1(3l)
B260 M4 E7-2800 v2 B260 M4 E7-4800 v2 B260 M4 E7-8800 v2 B260 M4 E7-4800 v3 B260 M4 E7-8800 v3	2.2(2e) 2.2(2e) 2.2(2e) 2.2(5d) 2.2(5d)	3.1(1e) 3.1(1e) 3.1(1e) 3.1(1e) 3.1(1e)	3.1(1e)	3.1(3l)
B260 M4 E7-4800 v4 B260 M4 E7-8800 v4	2.2(8b) 2.2(8b)	3.1(2b) 3.1(2b)	3.1(2b) 3.1(2b)	3.1(3l)
B420 M3 E5-4600 B420 M3 E5-4600 v2	2.2(1b) 2.2(2e)	3.1(1e) 3.1(1e)	3.1(1e)	3.1(3l)
B440 M2	2.2(1b)	3.1(1e)	3.1(1e)	3.1(3l)
B420 M4 E5-4600 v3 B420 M4 E5-4600 v4	2.2(5d) 2.2(8b)	3.1(1e) 3.1(2b)	3.1(1e) 3.1(2b)	3.1(3l) 3.1(3l)
B460 M4 E7-4800 v2 B460 M4 E7-8800 v2 B460 M4 E7-4800 v3 B460 M4 E7-8800 v3	2.2(2e) 2.2(2e) 2.2(5d) 2.2(5d)	3.1(1e) 3.1(1e) 3.1(1e) 3.1(1e)	3.1(1e)	3.1(3l)

Servers	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP FI	Minimum Software Version UCS 6332, 6332-16UPFI	Recommended Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI
	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2304	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2304
B460 M4 E7-4800 v4	2.2(8b)	3.1(2b)	3.1(2b)	3.1(3l)
B460 M4 E7-8800 v4	2.2(8b)	3.1(2b)		

Rack Servers

Table 13: Minimum Host Firmware Versions for Rack Servers

Servers	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332-16UP	Recommended Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI
	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2304	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2304
C22 M3 and M3L	2.2(1b)	3.1(1e)	3.1(1e)	3.1(3l)
C24 M3, M3L, and M3S2	2.2(1b)	3.1(1e)	3.1(1e)	3.1(3l)
C220 M3	2.2(1b)	3.1(1e)	3.1(1e)	3.1(3l)
C220 M4	2.2(3h)	3.1(1e)	3.1(1e)	3.1(3l)
C240 M3	2.2(1b)	3.1(1e)	3.1(1e)	3.1(3l)
C240 M4	2.2(3h)	3.1(1e)	3.1(1e)	3.1(3l)
C460 M4 E7-2800 v2	2.2(2e)	3.1(1e)	3.1(1e)	3.1(3l)
C460 M4 E7-4800 v2	2.2(2e)	3.1(1e)		
C460 M4 E7-8800 v2	2.2(2e)	3.1(1e)		
C460 M4 E7-4800 v3	2.2(5d)	3.1(1e)		
C460 M4 E7-8800 v3	2.2(5d)	3.1(1e)		

Servers	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332-16UP	Recommended Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI
	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2304	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2304
C460 M4 E7-8800 v4	2.2(8b)	3.1(2b)	3.1(2b)	3.1(3l)

Adapters

Table 14: Minimum Software Versions for Adapters

Adapters	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332-16UP	Recommended Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI
	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2304	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2304
UCSC-PCIE-C40Q-03 UCSC-MLOM-C40Q-03	2.2(7b)	3.1(1e)	3.1(1e)	3.1(3l)
UCS-VIC-M82-8P UCSB-MLOM-40G-01 UCSB-MLOM-PT-01	2.2(1b)	3.1(1e)	3.1(1e)	3.1(3l)
UCSB-MLOM-40G-03 UCSB-VIC-M83-8P UCSC-MLOM-CSC-02	2.2(3a)	3.1(1e)	3.1(1e)	3.1(3l)
UCSC-PCIE-CSC-02	2.2(1b)	3.1(1e)	3.1(1e)	3.1(3l)

Adapters	Minimum Software Version UCS 6200 Series FI UCS-IOM-2204 UCS-IOM-2208	Minimum Software Version UCS 6332, 6332-16UP UCS-IOM-2204 UCS-IOM-2208	Minimum Software Version UCS 6332, 6332-16UP UCS-IOM-2304	Recommended Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2304
UCSC-F-FIO-1000MP UCSC-F-FIO-1300MP UCSC-F-FIO-2600MP UCSC-F-FIO-5200MP	2.2(3a)	3.1(1e)	3.1(1e)	3.1(3l)
UCSB-FIO-1600MS UCSB-FIO-1300MS	2.2(3a)	3.1(1e)	3.1(1e)	3.1(3l)
UCSC-INVADER-3108 UCSC-NYTRO-200GB	2.2(3a)	3.1(1e)	3.1(1e)	3.1(3l)
UCSC-MLOM-C10T-02 UCSC-PCIE-C10T-02 UCSC-F-FIO-785M UCSC-F-FIO-365M UCSC-F-FIO-1205M UCSC-F-FIO-3000M UCSC-F-FIO1000PS UCSC-F-FIO1300PS UCSC-F-FIO2600PS UCSC-F-FIO5200PS UCSC-F-FIO-6400SS UCSC-F-FIO-3200SS	2.2(4b)	3.1(1e)	3.1(1e)	3.1(3l)
UCS-MEZ-QLG-03 UCSB-MEZ-ELX-03 N20-AQ0102 N20-AE0102	2.2(3a)	—	—	3.1(3l) [4]
UCS-PCIE-E14102B	2.2(7b)	—	—	3.1(3l)

Adapters	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332-16UP	Recommended Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI
	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2304	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2304
UCSC-PCIE-IQ10GF UCSC-PCIE-ID10GF UCSC-PCIE-ID40GF	—	—	3.1(2b)	3.1(3l)
UCSC-F-I80010 UCSC-F-I12003 UCSC-F-I160010 UCSC-F-I20003 UCS-PCI25-40010 UCS-PCI25-8003 UCS-PCI25-80010 UCS-PCI25-16003 UCSC-F-H19001 UCSC-F-H38001 UCS-SDHPCIE800GB UCS-SDHPCIE16TB UCS-PCI25-38001	—	—	3.1(2b)	3.1(3l)
UCSC-PCIE-QD32GF N2XX-AQPCI05 UCSC-PCIE-Q2672 UCSC-PCIE-BD32GF UCSC-PCIE-BS32GF UCSC-PCIE-E16002 N2XX-AEPCI05 UCSC-PCIE-ID10GC	—	—	3.1(3a)	3.1(3l)

[4] Support for UCS 6200 Series FI only.

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. The following is the list of other supported hardware:

Table 15: Supported Hardware for UCS 6332, UCS 6332-16UP Fabric Interconnects

Type	Details
Chassis	UCS-S3260 N20–C6508 UCSB-5108-DC UCSB-5108-AC2 UCSB-5108-DC2 UCSB-5108-HVDC
Fabric Interconnects	UCS 6332UP UCS 6332-16UP
Fabric Extenders	UCS 2208XP UCS 2204XP Cisco Nexus 2232PP Cisco Nexus 2232TM-E UCS-IOM-2304 Cisco Nexus 2348UPQ
Power Supplies	UCSB-PSU-2500HVDC UCSB-PSU-2500DC48 UCSC-PSU-930WDC UCSC-PSU2V2-930WDC UCSC-PSUV2-1050DC UCSC-PSU1-770W UCSC-PSU1-1050W UCSC-PSU2-1400 UCSC-PSU2V2-1400W UCSC-PSU2V2-650W UCSC-PSU2V2-1200W UCSB-PSU-2500ACPL UCSB-PSU-2500ACDV N20-PAC5-2500W

Note The 40G backplane setting is not applicable for 22xx IOMs.

Table 16: Supported Hardware for UCS 6200 Fabric Interconnects

Type	Details
Chassis	UCS-S3260 N20–C6508 UCSB-5108-DC UCSB-5108-AC2 UCSB-5108-DC2 UCSB-5108-HVDC
Fabric Interconnects	UCS 6248UP UCS 6296UP
Fabric Extenders	UCS 2208XP UCS 2204XP Cisco Nexus 2232PP Cisco Nexus 2232TM-E
Expansion Modules	UCS-FI-E16UP
Power Supplies	UCSB-PSU-2500HVDC UCSB-PSU-25004DC48 UCSC-PSU-930WDC UCSC-PSU2V2-930WDC UCSC-PSUV2-1050DC UCSC-PSU1-770W UCSC-PSU1-1050W UCSC-PSU2-1400 UCSC-PSU2V2-1400W UCSC-PSU2V2-650W UCSC-PSU2V2-1200W UCSB-PSU-2500ACPL UCSB-PSU-2500ACDV N20-PAC5-2500W

GB Connector Modules

The following is the list of Gb connector modules and supported cables:

Table 17: Supported Cables for GB Connector Modules

GB Connector Modules	Cables
40-GB for UCS 6300 Series Fabric Interconnects	CVR-QSFP-SFP10G QSFP-40G-CSR4 QSFP-40G-LR4 QSFP-40G-LR4-S QSFP-40G-SR-BD QSFP-40G-SR4 QSFP-40G-SR4-S QSFP-4SFP10G-CU1M QSFP-4SFP10G-CU3M QSFP-4SFP10G-CU5M QSFP-4X10G-AC10M QSFP-4X10G-AC7M QSFP-4X10G-AOC10M QSFP-4X10G-AOC1M QSFP-4X10G-AOC2M QSFP-4X10G-AOC3M QSFP-4X10G-AOC5M QSFP-4X10G-AOC7M QSFP-H40G-ACU10M QSFP-H40G-ACU7M QSFP-H40G-AOC10M QSFP-H40G-AOC15M QSFP-H40G-AOC1M QSFP-H40G-AOC2M QSFP-H40G-AOC3M QSFP-H40G-AOC5M QSFP-H40G-AOC7M QSFP-H40G-CU1M QSFP-H40G-CU3M QSFP-H40G-CU5M

GB Connector Modules	Cables
16-GB	DS-SFP-FC16G-LW DS-SFP-FC16G-SW
10-GB	SFP-10G-SR SFP-10G-LR SFP-H10GB-CU1M SFP-H10GB-CU3M SFP-H10GB-CU5M SFP-H10GB-ACU7M SFP-H10GB-ACU10M FET-10G [5]SFP-10G-AOC1M SFP-10G-AOC2M SFP-10G-AOC3M SFP-10G-AOC5M SFP-10G-AOC7M SFP-10G-AOC10M
8-GB (FC Expansion Module N10-E0060)	DS-SFP-FC8G-SW DS-SFP-FC8G-LW
4-GB (FC Expansion Module N10-E0080)	DS-SFP-FC4G-SW DS-SFP-FC4G-LW
1-GB	GLC-TE GLC-T (V03 or higher) GLC-SX-MM GLC-LH-SM

[5] Cisco 1225, 1227, and 1285 VIC cards are not supported with SFP-10G-AOC cables. SFP-10G-AOC cables are only supported for Cisco 1385 and 1387 VIC cards.

Cisco UCS Mini and Components

UCS Mini Supported Chassis

Chassis	Minimum Software Version	Recommended Software Version
UCSB-5108-AC2	3.0(1e)	3.1(3l)
UCSB-5108-DC2	3.0(2c)	3.1(3l)

UCS Mini Supported Blade and Rack Servers

Servers	Minimum Software Version	Recommended Software Version
B200 M3	3.0(1d)	3.1(3l)
B200 M4	3.0(2c)	3.1(3l)
B260 M4	3.1(2b)	3.1(3l)
B420 M3	3.0(2c)	3.1(3l)
B420 M4	3.1(1e)	3.1(3l)
B460 M4	3.1(2b)	3.1(3l)
B22 M3	3.0(2c)	3.1(3l)
C220 M3	3.0(1d)	3.1(3l)
C240 M3	3.0(1d)	3.1(3l)
C220 M4	3.0(2c)	3.1(3l)
C240 M4	3.0(2c)	3.1(3l)

UCS Mini Supported Adapters

Adapters	Minimum Software Version	Recommended Software Version
UCSC-PCIE-C40Q-03 UCSC-MLOM-C40Q-03	3.1(1e)	3.1(3l)
UCS-VIC-M82-8P UCSB-MLOM-40G-01 UCSB-MLOM-PT-01	3.0(1d)	3.1(3l)
UCSB-MLOM-40G-03 UCSB-VIC-M83P-8P UCSC-MLOM-CSC-02	3.0(2c)	3.1(3l)
UCSC-PCIE-CSC-02	3.0(1d)	3.1(3l)

UCS Mini Supported Fabric Interconnects

Fabric Interconnects	Minimum Software Version	Recommended Software Version
Cisco UCS 6324	3.1(1e)	3.1(3l)

UCS Mini Supported Fabric Extenders for Secondary Chassis

Fabric Extenders	Minimum Software Version	Recommended Software Version
UCS 2204 XP	3.1(1e)	3.1(3l)
UCS 2208 XP	3.1(1e)	3.1(3l)

UCS Mini Supported Power Supplies

Power Supplies	Minimum Software Version	Recommended Software Version
UCSB-PSU-2500ACDV UCSB-PSU-2500DC48 UCSC-PSU-930WDC UCSC-PSU2V2-930WDC UCSC-PSUV2-1050DC UCSC-PSU1-770W UCSC-PSU2-1400 UCSC-PSU2V2-1400W UCSC-PSU2V2-650W UCSC-PSU2V2-1200W	3.0(1e)	3.1(3l)

UCS Mini Supported Gb Connector Modules

We recommend that you use the current software version for Gb port speed connections. The following is the list of Gb connector modules and supported cables:

Gb Connector Modules	Cables
40-GB	QSFP-4SFP10G-CU1M QSFP-4SFP10G-CU3M QSFP-4SFP10G-CU5M QSFP-4X10G-AC7M QSFP-4X10G-AC10M QSFP-4X10G-AOC1M QSFP-4X10G-AOC2M QSFP-4X10G-AOC3M QSFP-4X10G-AOC5M QSFP-4X10G-AOC7M QSFP-4X10G-AOC10M

Gb Connector Modules	Cables
10-GB	SFP-10G-LR SFP-10G-LR-X SFP-10G-SR SFP-10G-SR-X SFP-H10GB-CU1M SFP-H10GB-CU3M SFP-H10GB-CU5M SFP-H10GB-ACU7M SFP-H10GB-ACU10M SFP-10G-AOC1M SFP-10G-AOC3M SFP-10G-AOC5M SFP-10G-AOC7M SFP-10G-AOC10M
8-GB	DS-SFP-FC8G-SW DS-SFP-FC8G-LW
4-GB	DS-SFP-FC4G-SW DS-SFP-FC4G-LW
1-GB	GLC-GE-T GLC-LH-SM GLC-SX-MM GLC-T (V03 or higher)

Modular Server and Components

The tables list the minimum server bundle recommended for this hardware in a mixed firmware configuration, assuming the infrastructure is at the recommended software version.

Important Cisco UCS Manager Release 3.1(2) and later releases do not support Cisco UCS M-Series Servers.

Chassis

Recommended minimum software versions do not consider mixed environments. To determine the minimum software version for your mixed environment, refer to "Cross-Version Firmware Support".

Chassis	Minimum Software Version	Recommended Software Version
UCSME-4308	2.5(1a)	3.1(1l)

Cartridges

To use a specific cartridge, Cisco UCS Manager, CMC, and the shared adapter must be upgraded to the recommended minimum software version for that cartridge.

Cartridges	Minimum Software Version	Recommended Software Version
UCSME-142-M4	2.5(1a)	3.1(1l)
UCSME-2814	2.5(2b)	3.1(1l)
UCSME-1414	2.5(2b)	3.1(1l)

Fabric Interconnect

Fabric Interconnect	Minimum Software Version	Recommended Software Version
UCS 6248UP	2.5(1a)	3.1(1l)
UCS 6296UP	2.5(1a)	3.1(1l)

Note Cisco UCS 6332 and UCS 6332-16UP Fabric Interconnects support is not available for Cisco M-Series Modular Servers.

Power Supply

Power Supply	Minimum Software Version	Recommended Software Version
UCSC-PSU2-1400W	2.5(1a)	3.1(1l)
UCSC-PSU2V2-1400W	2.5(2b)	3.1(1l)

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 18: Version Mapping

UCS Release	Catalog File Name	PIDs
3.1(1e)	ucs-catalog.3.1.1e.T.bin	

UCS Release	Catalog File Name	PIDs
		Blade GPU: UCSB-GPU-M6 GPU M60 adapter: UCSC-GPU-K80 **Note** Certain NVIDIA Graphics Processing Units (GPU) do not support Error Correcting Code (ECC) and vGPU together. Cisco recommends that you refer to the release notes published by NVIDIA for the respective GPU to know whether it supports ECC and vGPU together. Crypto Card: CSB-MEZ-INT8955 C240M4 NEBS SKU: UCSC-C240-M4SNEBS NVME SSD Drives: • UCS-SDHPCIE800GB Qlogic network adapters: • UCSC-PCIE-QNICBT • UCSC-PCIE-QNICSFP Cisco UCS VIC adapters: • UCSC-PCIE-C40Q-03 • UCSC-MLOM-C40Q-03 SX350 Fusion IO adaptor: • UCSC-F-S32002 • UCSC-F-S13002 • UCSC-F-S16002 • UCSC-F-S64002 Compute Cartridge: • UCSME-142L1-M5 • UCSME-142L2-M5 • UCSME-142M1-M5 • UCSME-142M2-M5 • UCSME-1414L1-M5 • UCSME-1414L2-M5 • UCSME-1414M1-M5

UCS Release	Catalog File Name	PIDs
		• UCSME-1414M2-M5

UCS Release	Catalog File Name	PIDs
3.1(1g)	ucs-catalog.3.1.1g.T.bin	

UCS Release	Catalog File Name	PIDs
		Cisco UCS B200 M4, C220 M4, and C240 M4 CPUs • UCS-CPU-E52699E • UCS-CPU-E52698E • UCS-CPU-E52697AE • UCS-CPU-E52697E • UCS-CPU-E52695E • UCS-CPU-E52690E • UCS-CPU-E52683E • UCS-CPU-E52680E • UCS-CPU-E52667E • UCS-CPU-E52660E • UCS-CPU-E52658E • UCS-CPU-E52650E • UCS-CPU-E52650LE • UCS-CPU-E52640E • UCS-CPU-E52637E • UCS-CPU-E52630E • UCS-CPU-E52630LE • UCS-CPU-E52623E • UCS-CPU-E52637E • UCS-CPU-E52620E • UCS-CPU-E52609E NVME SSD Drives • UCS-SDHPCIE1600GB [6] Memory • UCS-ML-1X324RU-A • UCS-ML-1X644RU-A • UCS-MR-1X081RV-A • UCS-MR-1X161RV-A

UCS Release	Catalog File Name	PIDs
		• UCS-MR-1X322RV-A • UCS-ML-1X324RV-A **Note** Requires Cisco UCS Manager Release 3.1(1h) or later releases for Cisco UCS B-Series servers. • UCS-ML-1X644RV-A **Note** Requires Cisco UCS Manager Release 3.1(1h) or later releases for Cisco UCS B-Series servers. Drives • UCS-SD400GBK9 • UCS-HD1T7KL12G • UCS-HD2T7KL12G • UCS-HD4T7KL12G • UCS-HD2T7KL6GA • UCS-HD10T7KL4K • UCS-HD4TBK9 • A03-D300GA2 • A03-D600GA2 • UCS-HDD900GI2F106 • UCS-SD16TBKS4-EV
3.1(1h)	ucs-catalog.3.1.1h.T.bin	Drives • UCS-SD480GBKS4-EV
3.1(1k)	—	—
3.1(1l)	—	—

UCS Release	Catalog File Name	PIDs
3.1(2b)	ucs-catalog.3.1.2b.T.bin	

UCS Release	Catalog File Name	PIDs
		Network Adaptors • UCSC-C3260-SIOC • UCSC-PCIE-ID10GF • UCSC-PCIE-ID40GF • UCSC-PCIE-IQ10GF CPUs • UCS-CPU-E5-4610E • UCS-CPU-E5-4620E • UCS-CPU-E5-4627E • UCS-CPU-E5-4640E • UCS-CPU-E5-4650E • UCS-CPU-E5-4655E • UCS-CPU-E5-4660E • UCS-CPU-E5-4667E • UCS-CPU-E5-4669E • UCS-CPU-E52650E • UCS-CPU-E74809E • UCS-CPU-E74820E • UCS-CPU-E74830E • UCS-CPU-E74850E • UCS-CPU-E78860E • UCS-CPU-E78867E • UCS-CPU-E78870E • UCS-CPU-E78880E • UCS-CPU-E78890E • UCS-CPU-E78891E • UCS-CPU-E78893E Memory • UCS-ML-1X324RU-A • UCS-ML-1X324RU-G

UCS Release	Catalog File Name	PIDs
		• UCS-ML-1X324RV-A • UCS-ML-1X644RU-G • UCS-MR-1X081RU-G • UCS-MR-1X082RZ-A • UCS-MR-1X161RV-A • UCS-MR-1X161RV-G • UCS-MR-1X162RU-A • UCS-MR-1X162RU-G • UCS-MR-1X162RV-A • UCS-MR-1X162RY-A • UCS-MR-1X322RU-G • UCS-MR-1X322RV-A • UCS-MR-2X162RY-E • UCS-MU-1X082RY-F Drives

UCS Release	Catalog File Name	PIDs
		• A03-D300GA2 • A03-D600GA2 • A03-D600GA2 • UCS-C3K-3XTSSD16 • UCS-C3K-3XTSSD32 • UCS-C3K-3XTSSD4 • UCS-C3K-3XTSSD8 • UCS-C3X60-G2SD12 • UCS-C3X60-G2SD160 • UCS-C3X60-G2SD48 • UCS-HD10T7KEM • UCS-HD12G10K9 • UCS-HD18G10K9 • UCS-HD2T7KL12G • UCS-HD2T7KL6GA • UCS-HD300G10K9 • UCS-HD4T12GK9 • UCS-HD4T7KL12G • UCS-HD600G15K9 • UCS-HD6T12GAK9 • UCS-HD6T12GK9 • UCS-HD6T7KEM • UCS-HD6T7KL4K • UCS-HD8T7KEM • UCS-HDD900GI2F106 • UCS-SD120GBE1K9 • UCS-SD16TB12S3-EP • UCS-SD16TBEK9 • UCS-SD16TBKS4-EV • UCS-SD200G0KS2-EP • UCS-SD200G12S3-EP

UCS Release	Catalog File Name	PIDs
		• UCS-SD400G0KS2-EP • UCS-SD400GBEK9 • UCS-SD480G12S3-EP • UCS-SD480GBE1K9 • UCS-SD600GBE3K9 • UCS-SD800G0KHY-EP • UCS-SD800G0KS2-EP • UCS-SD800G12S3-EP • UCS-SD800G12S4-EP • UCS-SD800GBEK9 • UCS-SD960GBE1K9 • UCS-SDHPCIE800GB • UCSC-C3160-400SSD Power Supply • UCSC-PSU1-1050W • UCSC-PSUV2-1050DC Storage Controllers

UCS Release	Catalog File Name	PIDs
		• UCS-C3K-M4RAID • UCS-PCI25-16003 • UCS-PCI25-38001 • UCS-PCI25-40010 • UCS-PCI25-80010 • UCS-PCI25-8003 • UCSC-C3X60-HBA • UCSC-C3X60-R1GB • UCSC-C3X60-R4GB • UCSC-F-H19001 • UCSC-F-H38001 • UCSC-F-I12003 • UCSC-F-I160010 • UCSC-F-I20003 • UCSC-F-I80010 • UCSC-PSAS12GHBA • UCSC-SAS12GHBA • UCSC-SAS9300-8E Server Platforms • HX240C-M4SX • HX220C-M4S
3.1(2c)	—	—
—	ucs-catalog.3.1.2e.T.bin	• UCS-SD480GBKS-EV • UCS-SD19TBKSS-EV

UCS Release	Catalog File Name	PIDs
3.1(2e)	ucs-catalog.3.1.2f.T.bin	CPU • UCS-CPU-E52699AE • UCS-CPU-E78894E Server Platforms • HXAF220C-M4S (C220 M4) • HXAF240C-M4SX (C240 M4SX)
3.1(2f)	ucs-catalog.3.1.2i.T.bin	—
3.1(2g)	ucs-catalog.3.1.2j.T.bin	—
3.1(2h)	ucs-catalog.3.1.2j.T.bin	—
3.1(3b)	ucs-catalog.3.1.3c.T.bin	—
3.1(3c)	—	—

UCS Release	Catalog File Name	PIDs
3.1(3d)	ucs-catalog.3.1.3e.T.bin	Drives: • UCS-HD8T7KL6GA • UCS-HD10T7KL6GA • UCS-S3260-G3SD24 • UCS-S3260-G3SD48 • UCS-S3260-G3SD160 • UCS-HY400GSAS3-EP • UCS-HY800GSAS3-EP • UCS-HY16TSAS3-EP • UCS-SD240GBKS4-EB • UCS-SD120GBKS4-EB • UCS-SD480GBKS4-EB • UCS-SD16TBKS4-EB NVMe drives: • UCSC-NVMEM4-H800 • UCSC-NVMEM4-H1600 • UCSC-NVME-H32003 • UCSC-NVME-H64003 • UCSC-NVME-H76801
3.1(3e)	ucs-catalog.3.1.3j.T.bin	—

UCS Release	Catalog File Name	PIDs
3.1(3f)	ucs-catalog.3.1.3m.T.bin	• UCS-HD10T7KL4KSM • UCS-HD12T7KL4KHM • UCS-HD12T7KL6GHA • UCS-HD8T7KL4KSM • UCS-HY19TIS3-EP • UCS-HY480GIS3-EP • UCS-S3260-3SSD16 • UCS-S3260-3SSD32 • UCS-S3260-3SSD4 • UCS-S3260-HD12T • UCS-S3260-HD12TR • UCS-S3260-NVM416 • UCS-S3260-NVM432 • UCS-S3260-NVM464 • UCS-S3260-NVM48 • UCS-SD16TH3-EP • UCS-SD19TIS3-EP • UCS-SD32TH3-EP • UCS-SD38TBIS6-EV • UCS-SD400GH3-EP • UCS-SD480GBIS6-EV • UCS-SD480GIS3-EP • UCS-SD800GH3-EP • UCS-SD960GBIS6-EV • UCS-SD960GIS3-EP
3.1(3h)	ucs-catalog.3.1.3n.T.bin	Drive: • UCS-S3260-TSD4K9
3.1(3j)	ucs-catalog.3.1.3p.T.bin	—
3.1(3k)	ucs-catalog.3.1.3q.T.bin	—
3.1(3l)	ucs-catalog.3.1.3q.T.bin	—

[6] For 1.6 TB HGST NVME drives, when used with B200-M4 blade servers, the minimum required board controller version is 12, which is bundled with Cisco UCS Manager Release 2.2(7b)B and 3.1(1g)B.

Upgrade and Downgrade Guidelines

Make sure to review detailed upgrade, downgrade guidelines and recommendations in Cisco UCS Manager Firmware Management guide, Release 3.1 from here: Cisco UCS Manager Configuration Guides

The following are a few reminders before you plan your upgrade to Cisco UCS Manager, Release 3.1:

- In a Cisco UCS domain with a Cisco UCS S3260 chassis, when you downgrade from Cisco UCS Manager Release 3.1(2b) to earlier releases, ensure that you decommission the Cisco UCS S3260 chassis. This is because the Cisco UCS S3260 chassis is supported only by Cisco UCS Manager Release 3.1(2b) and later releases.

  If you downgrade from Cisco UCS Manager Release 3.1(2b) to earlier releases without decommissioning the chassis, upgrade validation will fail and Cisco UCS Manager will prompt you to decommission the chassis before continuing with the downgrade operation.

- Auto-firmware upgrade is not supported in two different fabric Interconnect types in same cluster.
- When you download A bundle for your fabric Interconnect, you must download the correct A bundle specified for the fabric Interconnect type.
- If you have any of the deprecated hardware in your environment, the system will prevent upgrade to Cisco UCS Manager 3.1. See Deprecated Hardware, Software, and Third Party Adapters Support in Cisco UCS Manager, on page 20
- You must disable SNMP before downgrading from Cisco UCS Manager Release 3.1 to an earlier release, except in Cisco UCS Manager Release 2.2(6). The downgrade process does not begin until SNMP is disabled.
- Once **Compute Conn Policy** is set to **single-server-dual-sioc**, you cannot downgrade Cisco UCS Manager to any release earlier than 3.1(3a). Similarly, Cisco UCS Manager prevents BMC, CMC, and BIOS downgrade to any release earlier than 3.1(3a).
- If a Cisco UCS S3260 system has Dual HBA Controller then you cannot downgrade Cisco UCS Manager to any release earlier than 3.1(3a).
- You cannot downgrade Cisco UCS Manager, BMC, CMC, and BIOS to any release earlier than 3.1(3a) depending on the number of disk zoned to the controllers:

Controller Configuration	Is Downgrade Possible?
Two controllers in the server (one in optional I/O expander) or one controller in the server (in optional I/O expander) and at least one disk is zoned to the controller in the optional I/O expander.	No
Two controllers in the server (one in optional I/O expander) or one controller in the server (in optional I/O expander) and at least one disk is pre-provisioned to controller in the optional I/O expander.	No

Controller Configuration	Is Downgrade Possible?
Two controllers in the server (one in optional I/O expander) or one controller in the server (in any slot) and disk are not zoned or pre-prvosioned to the controller in optional I/O expander.	Yes

Security Fixes

The following security issues are resolved:

Release	Defect ID	CVE	Description
3.1(3l)	CSCve02433	CVE-2018-0314	A vulnerability in the Cisco Fabric Services (CFS) component of Cisco FXOS Software and Cisco NX-OS Software could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. The vulnerability exists because the affected software insufficiently validates Cisco Fabric Services packet headers when the software processes packet data. An attacker could exploit this vulnerability by sending a maliciously crafted Cisco Fabric Services packet to an affected device. A successful exploit could allow the attacker to cause a buffer overflow condition on the device, which could allow the attacker to execute arbitrary code on the 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 FXOS and NX-OS Software Cisco Fabric Services Arbitrary Code Execution Vulnerability

Release	Defect ID	CVE	Description
3.1(3l)	CSCve02787	CVE-2018-0308	A vulnerability in the Cisco Fabric Services component of Cisco FXOS Software and Cisco NX-OS Software could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. The vulnerability exists because the affected software insufficiently validates header values in Cisco Fabric Services packets. An attacker could exploit this vulnerability by sending a crafted Cisco Fabric Services packet to an affected device. A successful exploit could allow the attacker to cause a buffer overflow, which could allow the attacker to execute arbitrary code or cause a DoS condition. 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 FXOS and NX-OS Software Cisco Fabric Services Arbitrary Code Execution Vulnerability

Release	Defect ID	CVE	Description
3.1(3l)	CSCve41538	CVE-2018-0310	A vulnerability in the Cisco Fabric Services component of Cisco FXOS Software and Cisco NX-OS Software could allow an unauthenticated, remote attacker to obtain sensitive information from memory content, create a denial of service (DoS) condition, or execute arbitrary code as root. The vulnerability exists because the affected software insufficiently validates Cisco Fabric Services packet headers. An attacker could exploit this vulnerability by sending a crafted Cisco Fabric Services packet to an affected device. A successful exploit could allow the attacker to cause a buffer overflow or buffer overread condition in the Cisco Fabric Services component, which could allow the attacker to obtain sensitive memory content, create a DoS condition, or execute arbitrary code as root. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability. These advisories are available at the following links: Cisco FXOS and NX-OS Software Cisco Fabric Services Denial of Service Vulnerability Cisco FXOS and NX-OS Software Cisco Fabric Services Arbitrary Code Execution Vulnerability

Release	Defect ID	CVE	Description
3.1(3l)	CSCve41593	CVE-2018-0305	A vulnerability in the Cisco Fabric Services (CFS) component of Cisco FXOS Software and Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability exists because the affected software insufficiently validates Cisco Fabric Services packets when the software processes packet data. An attacker could exploit this vulnerability by sending a maliciously crafted Cisco Fabric Services packet to an affected device. A successful exploit could allow the attacker to force a NULL pointer dereference or cause a buffer overflow condition on the device, which could cause process crashes and result in a DoS condition on the 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 FXOS and NX-OS Software Cisco Fabric Services Denial of Service Vulnerability

Release	Defect ID	CVE	Description
3.1(3l)	CSCvg71290	CVE-2018-0291	A vulnerability in the Simple Network Management Protocol (SNMP) input packet processor of Cisco NX-OS Software could allow an authenticated, remote attacker to cause the SNMP application on an affected device to restart unexpectedly. The vulnerability is due to improper validation of SNMP protocol data units (PDUs) in SNMP packets. An attacker could exploit this vulnerability by sending a crafted SNMP packet to an affected device. A successful exploit could allow the attacker to cause the SNMP application to restart multiple times, leading to a system-level restart and a denial of service (DoS) condition. 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 NX-OS Software Authenticated Simple Network Management Protocol Denial of Service Vulnerability

Release	Defect ID	CVE	Description
3.1(3l)	CSCvp28016 CSCvp27917 CSCvp30013	CVE-2018-12126 CVE-2018-12127 CVE-2018-12130 CVE-2019-11091	

Release	Defect ID	CVE	Description
			Cisco UCS M3 and M4 servers and Hyperflex M4 servers are vulnerable to variants of exploits that use Microarchitectural Data Sampling (MDS) to gain access to data being processed in the CPU by other applications. • CVE-2018-12126 (Microarchitectural Store Buffer Data Sampling) affects store buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Manager release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. • CVE-2018-12127 (Microarchitectural Load Port Data Sampling) affects load buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Manager release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. • CVE-2018-12130 (Microarchitectural Fill Buffer Data Sampling) affects line fill buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Manager release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. • CVE-2019-11091 (Microarchitectural Data Sampling Uncacheable Memory) affects uncacheable memory in the CPU, and is addressed by applying the updated microcode included in the UCS Manager release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. This release includes BIOS revisions for the follwing servers: • Cisco UCS M4 servers and

Release	Defect ID	CVE	Description
			Hyperflex M4 servers that are based on Intel® Xeon® Processor E5 v3 and v4 Product Family processors • Cisco UCS M4 servers and Hyperflex M4 servers that are based on Intel® Xeon® Processor E7 v2 Product Family processors • Cisco UCS B-Series M3 Blade Servers that are based on Intel® Xeon® Sandy Bridge E5-2600 and Ivy Bridge E5 2600 v2 Product Family processors These BIOS revisions include the updated microcode that is a required part of the mitigation for these vulnerabilities.

Release	Defect ID	CVE	Description
3.1(3l)	CSCvr54413 CSCvr54414	• CVE-2019-0151 • CVE-2019-11137	

Release	Defect ID	CVE	Description
			Cisco UCS B-Series M4 servers that are based on Intel® processors are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs: • CVE-2019-0151 (CPU Local Privilege Escalation Advisory) affects certain Intel® 4th Generation Intel® Core™ Processors, 5th Generation Intel® Core™ Processors, 6th Generation Intel® Cores Processors, 7th Generation Intel® Core™ Processors, 8th Generation Intel® Core™ Processors, Intel® Xeon® Processors E3 v2/v3/v4/v5/v6 Family, Intel® Xeon® Processors E5 v3/v4 Family, Intel® Xeon® Processors E7 v3/v4 Family, Intel® Xeon® Scalable Processors 2nd Generation, Intel® Xeon® Scalable Processors, Intel® Xeon® Processors D-1500/D-2100), Intel® Xeon® Processors E-2100/E3100, and, Intel® Xeon® Processors W-2100/W-3100 when insufficient memory protection in Intel® TXT may allow a privileged user to potentially enable escalation of privilege through local access. This could result in bypassing Intel® TXT protections. • CVE-2019-11137 (BIOS 2019.2 IPU Advisory) affects 2nd Generation Intel® Xeon® Scalable Processors, Intel® Xeon® Scalable Processors, Intel® Xeon® Processor D Family, Intel® Xeon® Processor E5 v4 Family, Intel® Xeon® Processor E7 v4 Family, Intel® Atom® Processor C Series when insufficient input validation in the system firmware may allow a privileged user to potentially enable an escalation of privilege, denial of service, or information disclosure through local access. This release includes BIOS revisions for

Release	Defect ID	CVE	Description
			Cisco UCS B-Series M4 servers. These BIOS revisions include the updated microcode and SINIT ACM for Cisco UCS M4 servers, which are required parts of the mitigation for these vulnerabilities.
3.1(3l)	CSCvr54411	CVE-2019-0151	Cisco UCS B-Series M3 servers that are based on Intel® processors are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID: • CVE-2019-0151 (CPU Local Privilege Escalation Advisory) affects certain Intel® 4th Generation Intel® Core™ Processors, 5th Generation Intel® Core™ Processors, 6th Generation Intel® Cores Processors, 7th Generation Intel® Core™ Processors, 8th Generation Intel® Core™ Processors, Intel® Xeon® Processors E3 v2/v3/v4/v5/v6 Family, Intel® Xeon® Processors E5 v3/v4 Family, Intel® Xeon® Processors E7 v3/v4 Family, Intel® Xeon® Scalable Processors 2nd Generation, Intel® Xeon® Scalable Processors, Intel® Xeon® Processors D-1500/D-2100), Intel® Xeon® Processors E-2100/E3100, and, Intel® Xeon® Processors W-2100/W-3100 when insufficient memory protection in Intel® TXT may allow a privileged user to potentially enable escalation of privilege through local access. This could result in bypassing Intel® TXT protections. This release includes BIOS revisions for Cisco UCS B-Series M3 servers. These BIOS revisions include the updated SINIT ACM for Cisco UCS M3 servers, which is a required part of the mitigation for these vulnerabilities.

Release	Defect ID	CVE	Description
3.1(3k)	CSCvj59299 CSCvj59301	CVE-2018-3639 CVE-2018-3640	Cisco UCS M2 servers that are based on Intel® EX Series processors are vulnerable to variants of an exploit that uses CPU speculative processing and data cache timing to efficiently leak information, known as Spectre. CVE-2018-3639 (Spectre/Variant #4) and CVE-2018-3640 (Spectre/Variant #3a) are addressed by applying the updated processor microcode from Intel included in the server firmware bundle, and the relevant Operating System and Hypervisor patches from the appropriate vendors. This release includes BIOS revisions for Cisco UCS M2 B-Series blade servers that are based on Intel® EP Series processors. These BIOS revisions include the updated processor microcode that is a required part of the mitigation for CVE-2018-3639 (Spectre/Variant #4) and CVE-2018-3640 (Spectre/Variant #3a). **Important** This release does not include the updated processor microcode for Cisco UCS M2 C-Series rack-mount servers. For more information, please see the Cisco Security Advisory available here: CPU Side-Channel Information Disclosure Vulnerabilities: May 2018
3.1(3k)	CSCvq66225	CVE-2019-9836	On the Cisco UCS C-Series servers that are based on AMD EPYC™ processors, using the user-selectable AMD secure encryption feature on a virtual machine running the Linux operating system, an encryption key could be compromised by manipulating the encryption technology's behavior. This release includes the BIOS revision to mitigate this risk. For more information about this vulnerability, see https://www.amd.com/en/corporate/product-security.

Release	Defect ID	CVE	Description
3.1(3j)	CSCvm02934	CVE-2018-3615 CVE-2018-3620 CVE-2018-3646	Cisco UCS B-Series M2 servers are based on Intel® processors that are vulnerable to exploits that use CPU speculative processing and data cache timing to potentially identify privileged information. These exploits are collectively known as L1 Terminal Fault (L1TF). • CVE-2018-3615 (affecting SGX), also known as Foreshadow, is not known to affect any existing Cisco UCS servers because Cisco UCS M5 and earlier generation servers, and HyperFlex M5 and earlier generation servers do not use Intel® SGX technology. • CVE-2018-3620 (affecting OS/System Management Mode) and CVE-2018-3646 (affecting Virtual Machine Monitors) are referred to as L1 Terminal Fault attacks by Intel®. These vulnerabilities are mitigated by applying the updated processor microcode from Intel® included in the server firmware bundle, and the relevant Operating System and Hypervisor patches from the appropriate vendors. This release includes BIOS revisions for Cisco UCS M2 generation servers. These BIOS revisions include the updated processor microcode that is a required part of the mitigation for CVE-2018-3620 (OS/SMM) and CVE-2018-3646 (VMM). Operating System and Hypervisor patches from the appropriate vendors may also be required to mitigate these vulnerabilities. For more information, please see the Cisco Security Advisory available here: CPU Side-Channel Information Disclosure Vulnerabilities: August 2018

Release	Defect ID	CVE	Description
3.1(3j)	CSCvm03356	CVE-2018-3615 CVE-2018-3620 CVE-2018-3646	Cisco UCS B-Series M3 servers and C-Series M3 servers are based on Intel® processors that are vulnerable to exploits that use CPU speculative processing and data cache timing to potentially identify privileged information. These exploits are collectively known as L1 Terminal Fault (L1TF). • CVE-2018-3615 (affecting SGX), also known as Foreshadow, is not known to affect any existing Cisco UCS servers because Cisco UCS M5 and earlier generation servers, and HyperFlex M5 and earlier generation servers do not use Intel® SGX technology. • CVE-2018-3620 (affecting OS/System Management Mode) and CVE-2018-3646 (affecting Virtual Machine Monitors) are referred to as L1 Terminal Fault attacks by Intel®. These vulnerabilities are mitigated by applying the updated processor microcode from Intel® included in the server firmware bundle, and the relevant Operating System and Hypervisor patches from the appropriate vendors. This release includes BIOS revisions for Cisco UCS M3 generation servers. These BIOS revisions include the updated processor microcode that is a required part of the mitigation for CVE-2018-3620 (OS/SMM) and CVE-2018-3646 (VMM). Operating System and Hypervisor patches from the appropriate vendors may also be required to mitigate these vulnerabilities. For more information, please see the Cisco Security Advisory available here: CPU Side-Channel Information Disclosure Vulnerabilities: August 2018

Release	Defect ID	CVE	Description
3.1(3j)	CSCvm03351	CVE-2018-3615 CVE-2018-3620 CVE-2018-3646	Cisco UCS B-Series M4 servers, C-Series M4 servers, S3260 M4 storage servers, and HyperFlex M4 servers are vulnerable to exploits that use CPU speculative processing and data cache timing to potentially identify privileged information. These exploits are collectively known as L1 Terminal Fault (L1TF). • CVE-2018-3615 (affecting SGX), also known as Foreshadow, is not known to affect any existing Cisco UCS servers because Cisco UCS M5 and earlier generation servers, and HyperFlex M5 and earlier generation servers do not use Intel® SGX technology. • CVE-2018-3620 (affecting OS/System Management Mode) and CVE-2018-3646 (affecting Virtual Machine Monitors) are referred to as L1 Terminal Fault attacks by Intel®. These vulnerabilities are mitigated by applying the updated processor microcode from Intel® included in the server firmware bundle, and the relevant Operating System and Hypervisor patches from the appropriate vendors. This release includes BIOS revisions for Cisco UCS M4 generation servers. These BIOS revisions include the updated processor microcode that is a required part of the mitigation for CVE-2018-3620 (OS/SMM) and CVE-2018-3646 (VMM). Operating System and Hypervisor patches from the appropriate vendors may also be required to mitigate these vulnerabilities. For more information, please see the Cisco Security Advisory available here: CPU Side-Channel Information Disclosure Vulnerabilities: August 2018

Release	Defect ID	CVE	Description
3.1(3j)	CSCvd36971	CVE-2017-3883	A vulnerability in the authentication, authorization, and accounting (AAA) implementation of Cisco Firepower Extensible Operating System (FXOS) and NX-OS System Software could allow an unauthenticated, remote attacker to cause an affected device to reload. The vulnerability occurs because AAA processes prevent the NX-OS System Manager from receiving keepalive messages when an affected device receives a high rate of login attempts, such as in a brute-force login attack. System memory can run low on the FXOS devices under the same conditions, which could cause the AAA process to unexpectedly restart or cause the device to reload. An attacker could exploit this vulnerability by performing a brute-force login attack against a device that is configured with AAA security services. A successful exploit could allow the attacker to cause the affected device to reload. Cisco has now integrated the fix for this vulnerability on the UCS-FI-M-6324 platform (on UCS-FI-62xx and UCS-FI-63xx, the fix was integrated in Release 3.2(3a) already). Additionally, a remaining corner case that allowed attackers to connect using a valid password while the login block window is still active, has been addressed on all Fabric Interconnect platforms now. This advisory is available at the following link: Cisco FXOS and NX-OS System Software Authentication, Authorization, and Accounting Denial of Service Vulnerability

Release	Defect ID	CVE	Description
3.1(3j)	CSCvj59299	CVE-2018-3639 CVE-2018-3640	Cisco UCS M2 servers that are based on Intel® EP Series processors are vulnerable to variants of an exploit that uses CPU speculative processing and data cache timing to efficiently leak information, known as Spectre. CVE-2018-3639 (Spectre/Variant #4) and CVE-2018-3640 (Spectre/Variant #3a) are addressed by applying the updated processor microcode from Intel included in the server firmware bundle, and the relevant Operating System and Hypervisor patches from the appropriate vendors. This release includes BIOS revisions for Cisco UCS M2 B-Series blade servers that are based on Intel® EP Series processors. These BIOS revisions include the updated processor microcode that is a required part of the mitigation for CVE-2018-3639 (Spectre/Variant #4) and CVE-2018-3640 (Spectre/Variant #3a). **Important** This release does not include the updated processor microcode for Cisco UCS M2 C-Series rack-mount servers. For more information, see the Cisco Software Advisory at: CPU Side-Channel Information Disclosure Vulnerabilities: May 2018

Release	Defect ID	CVE	Description
3.1(3j)	CSCvj54880	CVE-2018-3639 CVE-2018-3640	Cisco UCS M3 servers are based on Intel® processors that are vulnerable to variants of an exploit that uses CPU speculative processing and data cache timing to efficiently leak information, known as Spectre. CVE-2018-3639 (Spectre/Variant #4) and CVE-2018-3640 (Spectre/Variant #3a) are addressed by applying the updated processor microcode from Intel included in the server firmware bundle, and the relevant Operating System and Hypervisor patches from the appropriate vendors. This release includes BIOS revisions for Cisco UCS M3 generation servers. These BIOS revisions include the updated processor microcode that is a required part of the mitigation for CVE-2018-3639 (Spectre/Variant #4) and CVE-2018-3640 (Spectre/Variant #3a). For more information, see the Cisco Software Advisory at: CPU Side-Channel Information Disclosure Vulnerabilities: May 2018

Release	Defect ID	CVE	Description
3.1(3j)	CSCvj54847 CSCvj54187	CVE-2018-3639 CVE-2018-3640	Cisco UCS M4 servers and Hyperflex M4 servers are based on Intel® processors that are vulnerable to variants of an exploit that uses CPU speculative processing and data cache timing to efficiently leak information, known as Spectre. CVE-2018-3639 (Spectre/Variant #4) and CVE-2018-3640 (Spectre/Variant #3a) are addressed by applying the updated processor microcode from Intel included in the server firmware bundle, and the relevant Operating System and Hypervisor patches from the appropriate vendors. This release includes BIOS revisions for Cisco UCS M4 and Hyperflex M4 generation servers. These BIOS revisions include the updated processor microcode that is a required part of the mitigation for CVE-2018-3639 (Spectre/Variant #4) and CVE-2018-3640 (Spectre/Variant #3a). For more information, see the Cisco Software Advisory at: CPU Side-Channel Information Disclosure Vulnerabilities: May 2018

Release	Defect ID	CVE	Description
3.1(3h)	CSCvh31576 CSCvh51796	• CVE-2017-5753 • CVE-2017-5715 • CVE-2017-5754	Cisco UCS B-Series and C-Series M2 servers are based on Intel® Xeon® 5500, 5600, and E*x* series processors that are vulnerable to variants of exploits that use CPU speculative processing and data cache timing to potentially identify privileged information. These exploits are collectively known as Spectre and Meltdown. • CVE-2017-5753 (Spectre/Variant 1) is addressed by applying relevant Operating System and Hypervisor patches from the appropriate vendors. • CVE-2017-5715 (Spectre/Variant 2) is addressed by applying the updated microcode included in the UCS Manager release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. • CVE-2017-5754 (Meltdown) is addressed by applying the relevant Operating System patches from the appropriate vendors. This release includes BIOS revisions for Cisco UCS M2 generation servers. These BIOS revisions include the updated microcode that is a required part of the mitigation for CVE-2017-5715 (Spectre/Variant 2). For more information, please see the Cisco Security Advisory at: CPU Side-Channel Information Disclosure Vulnerabilities
3.1(3f)	CSCve59744	CVE-2017-15361	The vulnerability related to TPM 2.0 is addressed.

Release	Defect ID	CVE	Description
3.1(3f)	CSCvg97965, CSCvg97979, CSCvg98015	• CVE-2017-5753 • CVE-2017-5715 • CVE-2017-5754	Cisco UCS and Hyperflex servers are based on Intel processors that are vulnerable to exploits that use CPU speculative processing and data cache timing to potentially identify privileged information. These exploits are collectively known as Spectre and Meltdown. • CVE-2017-5753 Spectre/Variant 1 – is addressed by applying relevant Operating System and Hypervisor patches from the appropriate vendors. • CVE-2017-5715 Spectre/Variant 2 – is addressed by applying the updated microcode included in the UCS Manager release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. • CVE-2017-5754 Meltdown – is addressed by applying the relevant Operating System patches from the appropriate vendors. This release includes the BIOS revisions for Cisco UCS M3 and M4 and Hyperflex M4 generation servers that include the updated microcode that is a required part of the mitigation for CVE-2017-5715 (Spectre/Variant 2). For more information, please see the Cisco Security Advisory at: CPU Side-Channel Information Disclosure Vulnerabilities

Release	Defect ID	CVE	Description
3.1(3a)	CSCvb48644	• CVE-2016-2177 • CVE-2016-2178 • CVE-2016-2179 • CVE-2016-2180 • CVE-2016-2181 • CVE-2016-2182 • CVE-2016-2183 • CVE-2016-6302 • CVE-2016-6303 • CVE-2016-6304 • CVE-2016-6306 • CVE-2016-7052	The latest CiscoSSL 6.1.188-fips (corresponding to OpenSSL 1.0.2k, and detailed in CSCvc94686) now automatically fixes the OpenSSL vulnerabilities identified by one or more of the Common Vulnerability and Exposures (CVE) IDs listed.
3.1(2e)	CSCvb85544	CVE-2016-5195	The vulnerability for a race condition that existed in the memory manager of the Linux kernel has been fixed.
3.1(2b)	CSCuz91623	CVE-2016-6402	The vulnerability associated with insufficient sanitization of user supplied input at the CLI on Cisco UCS Manager and UCS 6200 Fabric Interconnects is resolved.
3.1(1l)	CSCvb85544	CVE-2016-5195	The vulnerability for a race condition that existed in the memory manager of the Linux kernel has been fixed.
3.1(1k)	CSCuz92668	CVE-2016-4957, CVE-2016-4953, CVE-2016-4954, CVE-2016-4955, CVE-2016-4956	Vulnerabilities related to NTPd are fixed.

Release	Defect ID	CVE	Description
3.1(1e)	CSCuj84274	CVE-2013-4786	The vulnerability in Cisco Integrated Management Controller (CIMC) on the Cisco Unified Computing System Series Platforms associated with unauthenticated access is resolved.
	CSCut46044	CVE-2015-0291, CVE-2015-0204, CVE-2015-0290, CVE-2015-0207, CVE-2015-0286, CVE-2015-0208, CVE-2015-0287, CVE-2015-0289, CVE-2015-0292, CVE-2015-0293, CVE-2015-1787, CVE-2015-0285, CVE-2015-0288	Vulnerabilities related to OpenSSL are fixed.
	CSCup58725	CVE-2007-6514, CVE-2007-1741, CVE-2007-1742, CVE-2007-1743, CVE-2008-0455, CVE-2008-0456, CVE-2006-4110, CVE-2013-6438, CVE-2014- 0098, CVE-2014-3470, CVE-2010-2054, CVE-2010-1937, CVE-2010-5298, CVE-2014-0076, CVE-2014-0195, CVE-2014-0198, CVE-2014-0221, CVE-2014-0224, CVE-2014- 3470, CVE-2011-3389	Vulnerabilities associated with SBLIM-SFCB Multiple Buffer Overflow are fixed.
	CSCux00285		Security issues related to third party alerts are fixed.

Release	Defect ID	CVE	Description
		CVE-2011-2898, CVE-2014-6271, CVE-2014-7169, CVE-2014-6271, CVE-2014-7169, CVE-2014-7187, CVE-2014-6277, CVE-2011-0207, CVE-2012-0207, CVE-2011-4131, CVE-2014-2523, CVE-2012-3400, CVE-2012-1148, CVE-2011-4077, CVE-2012-0038, CVE-2014-4699, CVE-2014-0205, CVE-2013-1943, CVE-2012-4444, CVE-2012-2136, CVE-2012-0876, CVE-2014-1690, CVE-2011-4325, CVE-2012-2133, CVE-2013-4220, CVE-2012-1090, CVE-2012-2373, CVE-2012-2745, CVE-2011-3363, CVE-2012-1088, CVE-2012-1146 CVE-2012-2372, CVE-2012-3412, CVE-2012-3410, CVE-2012-3410, CVE-2012-4565, CVE-2012-5374, CVE-2013-0311, CVE-2014-7186, CVE-2011-1083, CVE-2011-3359, CVE-2012-1601, CVE-2012-2121, CVE-2012-2119, CVE-2012-3375, CVE-2012-4467, CVE-2009-3720, CVE-2009-3560, CVE-2013-1860, CVE-2012-0045, CVE-2013-1796, CVE-2012-3430, CVE-2012-2313, CVE-2012-4530, CVE-2012-1568, CVE-2012-5375	

Libfabric and Open MPI

Cisco usNIC support in the Libfabric and Open MPI open source packages is readily available from their community web sites (http://libfabric.org/ and http://www.open-mpi.org/, respectively).

Cisco UCS Manager Release 3.1(3) and later releases no longer include Open MPI binary packages. Future UCS software driver bundles distributed through the usual Cisco software channels may not include binaries for the libfabric packages. Cisco engineers continue to be active, core contributors in both the Libfabric and Open MPI communities, and will actively develop and support users through the usual community or commercial ISV support mechanisms (e.g., IBM Spectrum MPI).

Resolved Caveats

The resolved bugs for a release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains up-to-date information about bugs and vulnerabilities in this product and other Cisco hardware and software products.

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

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

Resolved Caveats in Release 3.1(3l)

The following caveats are resolved in Release 3.1(3l):

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvo49554	When a blade server is connected to ports 27-32 on a UCS 6332 Fabric Interconnect, or ports 35-40 on a UCS 6332-16UP Fabric Interconnect, numerous pings are lost during Fabric Interconnect reboot. This issue is resolved.	3.1(3h)A	3.1(3l)A
CSCvr67027	When upgrading Red Hat Linux on a Cisco UCS Manager integrated S3260 M4 rack server with UCS-C3K-M4RAID RAID controller running driver 07.702.06.00-rh2, the boot drive becomes inoperable. This issue is resolved.	3.1(3h)C	3.1(3l)C
CSCvf03280	When Cisco Fabric Services (CFS) distribution is enabled on UCS 6200 Series Fabric Interconnects, the Fabric Interconnect may reload due to a CFS process crash. This issue has been resolved.	3.1(3a)A	3.1(3l)A
CSCvs43658	When Cisco Fabric Services (CFS) distribution wass enabled on UCS Fabric Interconnects and the Infrastructure bundle was upgraded, both Fabric Interconnects rebooted continuously due to `CFS hap reset`. This issue has been resolved.	3.1(3k)A	3.1(3l)A

Resolved Caveats in Release 3.1(3k)

The following caveats are resolved in Release 3.1(3k):

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvk71319	The message queue may become full and if the VIM misses a heartbeat can result in VIM process crash.	3.1(3h)A	3.1(3k)A
CSCvj10772	Multicast traffic no longer drops on some Veths. The affected multicast group(s) are seen in the software but absent in the hardware.	3.1(3h)A	3.1(3k)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvk51589 CSCvk73712 CSCvk75400	Cisco UCS 6200 and 6300 Series Fabric Interconnects no longer reloads with the message: Reset triggered due to HA policy of Reset. This error may occur if the message queue becomes full.	3.1(3h)A	3.1(3k)A
CSCvh66141	When accessing KVM directly without first logging into UCS Manager, KVM will fail to launch if you are using non-native authentication.	3.1(3a)B	3.1(3k)B

Resolved Caveats in Release 3.1(3j)

The following caveats are resolved in Release 3.1(3j):

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvi98058	New OS installation in UEFI mode and BIOS version 2.2.6f.0 no longer fails.	3.1(3h)B	3.1(3j)A
CSCvi96785	On UCS 6332-16UP and 6332 fabric interconnects, the file system was corrupted and the **show logging** log or **show logging nvram** log contained a message with the term "EXT3-fs error". The fix in Cisco UCS Manager Release 3.1(3j) prevents this issue from occurring.	3.2(2b)A	3.1(3j)A 3.2(3g)
CSCvg64592 CSCvh17112 CSCvh11759	Rack servers integrated with 6200 Series FI, 6300 Series FIs, and 6324 FIs have connectivity after reboot of the subordinate FI, if the VLAN range (expressed as a string of characters) applied on a port-profile exceeds 255 characters.	3.1(3c)A	3.1(3j)A 3.2(3a)A
CSCvj63400 CSCvj88019 CSCvj88844	On UCS 6200 Series FIs, 6300 Series FIs and 6324 FIs running Cisco UCS Manager Release 3.2(2c), IOMs crashed with reset reason vic_proxy hap and generated a core. This happened when there was an invalid memory access. This issue has been resolved.	3.2(2c)A	3.1(3j)A, 3.2(3e)A
CSCvd54116	Setting a custom cipher suite for UCS Manager no longer results in a handshake failure error message when attempting to open a Java login to UCSM or a KVM session to a blade server.	2.2(8c)A	3.1(3j) 3.2(3g)A
CSCvj83780	Under specific low write and long idle time workloads, the following SATA SSDs no longer show read errors: • UCS-M2-240GB • HX-M2-240GB	3.2(2b)B	3.1(3j)B3.2(3e)B

Resolved Caveats in Release 3.1(3h)

The following caveats are resolved in Release 3.1(3h):

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvh60861	In a UCS domain running Cisco UCS Manager Release 3.1(x) or 3.2(x) code with UCS B200 M2 or B250 M2 servers, using a Host Firmware Package to perform a BIOS firmware upgrade from Release 2.5(x) or earlier versions to Release 3.1(x) or later versions no longer fails.	3.2(2b)A	3.1(3h)A

Resolved Caveats in Release 3.1(3f)

The following caveats are resolved in Release 3.1(3f)

Table 19: Resolved Caveats in Release 3.1(3f)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvb88279	Boot speeds are no longer slow when using a storage profile for pool LUNs on EMC VNX arrays.	3.1(2b)B	3.1(3f)B
CSCvh64120	DME no longer crashes after an upgrade to 3.1(3) or 3.2(2).	3.1(3a)A	3.1(3f)A
CSCvh22485	After a vMotion or virtual machine migration in a VMFEX setup, virtual machines were unable to receive broadcast or multicast packets, including ARP packets. The issue has been resolved.	2.2(8g)A	3.1(3f)A
CSCvg44307	Stale entries in IOM no longer cause a communication failure within the same VLAN and fabric interconnect.	2.2(4b)A	3.1(3f)A
CSCuw09993	ESXi no longer reports a fatal error while loading /s.v00 during the "Loading VMware Hypervisor" Screen.	2.2(3a)B	3.1(3f)B
CSCvh56396	mgmt0 IP now appears in the command "show ip interface brief vrf management" or "show run interface mgmt0" from connect nxos.	3.1(3e)A	3.1(3f)A
CSCve08388	A failure to update the local disk firmware image no longer occurs.	3.1(3c)A	3.1(3f)A
CSCve68431	UEFI Boot Parameters are now applied on B200 M3 and M4 servers with 3.1(2f).	3.1(2f)B	3.1(3f)B
CSCvf36433	Matrox G200e driver installation no longer produces an error on Windows 2016.	3.1(3a)C	3.1(3f)C
CSCvf50470	Cisco VIC adapter no longer displays an Exchange Allocation Failure and WQ Errors with fibre channel traffic.	3.1(3a)B	3.1(3f)B

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvf59328	TASK_SET_FULL SCSI response is no longer mishandled by FNIC.	1.6(0.25)	3.1(3f)B
CSCvg25428	Call Home Alert messages are no longer generated for weekly occurences of CIMC cores.	3.1(1h)C	3.1(3f)C
CSCvg99433	On UCS Mini, a fabric interconnect reboot no longer occurs from a QoS Buffer-Stuck error.	3.1(1e)A	3.1(3f)A
CSCvg98077	A TPM firmware update no longer fails if a UCS Manager event interrupts the process.	2.2(8i)B	3.1(3f)B
CSCvh07966	Firmware update no longer fails for Nvidia P100.	3.1(3d)C	3.1(3f)C
CSCvg88563	Both sockets of the Rack Server with UCSC-GPU-M60 now display the same firmware version.	3.1(3d)A	3.1(3f)A

Resolved Caveats in Release 3.1(3e)

The following caveats are resolved in Release 3.1(3e)

Table 20: Resolved Caveats in Release 3.1(3e)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvf59328	The fNIC no longer reports DATA_CNT_MISMATCH when the TASK_SET_FULL SCSI command is received from the storage array.	3.1(1e)	3.1(3e)
CSCvf50470	Server no longer loses FC connectivity with the datastore.	3.1(3a)	3.1(3e)

Resolved Caveats in Release 3.1(3d)

The following caveats are resolved in Release 3.1(3d)

Table 21: Resolved Caveats in Release 3.1(3d)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCve23500	Cisco UCS B200 M4 Blade Server no longer crashes with SD Card Connectivity issues.	2.2(3d)B	3.1(3d)B
CSCve30154	Cisco UCS B200 M4 Blade Server no longer fails to boot from the SD card mirror after the primary SD card fails.	3.1(2e)B	3.1(3d)B
CSCve34690	A FlexFlash Failure no longer reports a "missing" fault for functional SD cards.	3.1(2b)A	3.1(3d)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCve41380	The operating system no longer fails to boot when one of the SD cards in a RAID 1 configuration is inoperable.	3.1(1h)B	3.1(3d)B
CSCvd54828	The RAID controller encounters an error and resets. This happens when you use an external SATA solid state drive (SSD) and not an SAS SSD.	3.0(3a)C	3.1(3d)C

Resolved Caveats in Release 3.1(3c)

The following caveats are resolved in Release 3.1(3c)

Table 22: Resolved Caveats in Release 3.1(3c)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCve14926	A configuration error no longer occurs while associating a service profile with UCSC-C240M4-SX or UCSC-C240-M4L servers, under the following conditions: • The server has internal SSD(s) in slot 1 and 2 of the internal riser card, which are managed by the onboard PCH controller • The server has disks in external slot 1 and slot 2, which are managed by PCI slot based storage controller • The disk group policy, configured in the service profile, is set as **Disk Group Configuration (Manual)** • External disks 1 and 2 are selected in the manual disk group policy	3.1(1e)A	3.1(3c)A
CSCve35785	The SNMP process no longer crashes on UCS after an upgrade due to high memory usage.	3.1(3a)A	3.1(3c)A
CSCvf07449	The firmware update for the LSI 9300-8e controller no longer fails. After the update, the firmware version of the controller and the firmware version of the host firmware package are same.	3.1(3a)A	3.1(3c)A
CSCvf18955	During clustering, if one FI runs Release 3.1(3) and the other FI runs any release earlier than Release 3.1(3), an error message indicating that the local "Admin" password is incorrect, or that the authentication mode of the working fabric is not set to "Local" is no longer displayed.	3.1(3a)A	3.1(3c)A

Resolved Caveats in Release 3.1(3b)

The following caveats are resolved in Release 3.1(3b)

Table 23: Resolved Caveats in Release 3.1(3b)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCve30332	UCS Manager no longer becomes unresponsive when a Service Profile is associated with a server.	3.1(3a)A	3.1(3b)A
CSCve15708	UCS domain registration no longer fails on UCS firmware when using the IPv6 address of UCS Central.	3.1(3a)A	3.1(3b)A
CSCve06789	A service profile creation no longer fails with the SAN connectivity policy using vHBA when it is created with a redundancy pair.	3.1(3a)A	3.1(3b)A
CSCve41254	LUN creation no longer fails using Local Disk policy with RAID 60 mode in rack servers.	3.1(3a)A	3.1(3b)A
CSCve46288	UCS S3260 storage controller upgrade no longer fails for M3 servers during upgrades.	3.1(3a)A	3.1(3b)A
CSCvd91302	UCS Mini and the Fabric Interconnect no longer looses connection after a change in the MTU value in BM and DQ.	3.1(1e)A	3.1(3b)A
CSCve13711	While upgrading UCS Manager, the remote fabric interconnect no longer continuously reboots with a PCIe Device-Cisco Donner error.	3.1(3a)A	3.1(3b)A
CSCva31113	After a fabric interconnect reboot, a file system corruption no longer occurs on systems that contain an Indilinx controller.	2.2(1b)A	3.1(3b)A

Resolved Caveats in Release 3.1(3a)

The following caveats are resolved in Release 3.1(3a):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvc99135	The UCS Fabric Interconnect generates IGMP proxy reports where the source mac address of the data packets is replaced by the Fabric Interconnect, but the IP address is 0.0.0.0. Thus, multiple entries are not created in the IP-mac table for the IP in the uplink switch. Hence, there is no end point movement.	3.1(1e)B	3.1(3a)B
CSCuz76350	Cisco B260 or B460 M4 servers running RHEL 6.7 no longer become unresponsive when booting with all the DIMM slots fully populated.	3.1(2b)B	3.1(3a)B
CSCvb96124	After changes are made to the QoS policy on a Cisco UCS 6332 Fabric Interconnect, the primary FI is not rebooted until Pending Activities are acknowledged.	3.1(2b)A	3.1(3a)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvb14641	Power policies are no longer out of synchronization between Cisco UCS Manager and CMC after the master IOM is rebooted.	3.0(2c)A	3.1(3a)A

CSCvd24782	When the poweroff module was available for less than 15 seconds, all of the poweron commands timed out. The poweroff module <module_number> was then seen in the list of installed features on the FI through NXOS:
	`version 5.2(3)N2(2.27b)`
	`feature fcoe`
	`poweroff module 4`
	The module appeared to no longer work after it rebooted.
	This issue no longer occurs.
		3.1(1e)A	3.1(3a)A

CSCvb88279	On EMC VNX arrays, when pool-based LUNs with a frame size of 512 bytes from non-owning SPs are used, booting to non-owning SPs is no longer slow.	3.1(2b)B	3.1(3a)B
CSCvb52847	On a B200 M4 blade platform, instead of a NVMe plane, if RAID card is plugged in, then the /var/log/messages file no longer shows "Mux write error" messages. Apart from /var/log/message flood, no functional impact to normal storage operations are noticed.	3.1(2b)B	3.1(3a)B 3.1(2f)B

Resolved Caveats in Release 3.1(2h)

The following caveats are resolved in Release 3.1(2h).

Table 24: Resolved Caveats in Release 3.1(2h)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCuv43292	The fabric interconnect no longer crashes due to a sleeping function called within an interrupt context.	Both 2.2(4a)A and 2.2(5a)A are affected but not 2.2(6)A, 2.2(7)A, and 2.2(8)A.	3.1(2h)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCva31113	After a fabric interconnect reboot, a file system corruption no longer occurs on systems that contain an Indilinx controller.	2.1(1a)A	3.1(2h)A
CSCva89402	An incorrect fault is no longer generated in UCS Manager when the power supply input source is "unknown".	3.1(1e)B	3.1(2h)B
CSCvb14641	Power policies are no longer out of synchronization between Cisco UCS Manager and CMC after the master IOM is rebooted.	3.0(2c)A	3.1(2h)A
CSCvb61558	UCSB-PSU-2500ACDV no longer displays incorrect power readings in the PSMI register.	3.1(1e)A	3.1(2h)A
CSCvb92941	UCS-IOM-2304 no longer fails to capture kernel cores in the obfl_raw partition.	3.1(1e)A	3.1(2h)A
CSCvb93881	IOM 2300 and UCSB-5108-AC2 chassis no longer displays the fault F0409 "Thermal condition on chassis x is upper-critical". **Note** This has no operational impact but could generate call home alerts.	3.1(1g)A	3.1(2h)A
CSCvd56914	Microcode was added for Broadwell and Haswell EX processors support.	3.1(2b)B	3.1(2h)B
CSCvd68198	Microcode was added for E5 Xeon v4 Processor support.	3.1(2b)B	3.1(2h)B
CSCvd80748	For Cisco B260 or B460 Blade servers, the enable COD setting no longer causes an incorrect microcode version to appear.	3.1(2b)B	3.1(2h)B
CSCvd91302	UCS Mini and the Fabric Interconnect no longer loses connection after a change in the MTU value in BM and DQ.	3.1(1e)A	3.1(2h)A
CSCvd93200	A random reboot due to a spinlock lockup no longer occurs on Cisco UCS 2304.	3.1(1e)A	3.1(2h)A

Resolved Caveats in Release 3.1(2g)

The following caveats are resolved in Release 3.1(2g)

Table 25: Resolved Caveats in Release 3.1(2g)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCva67630	False SER errors no longer occurs for FP ternary content addressable memory (TCAM) tables for Cisco UCS 6300 Series Fabric Interconnects.	3.1(1g)A	3.1(2g)A
CSCvb68147	The IOM no longer goes offline when the host interface links are down and under constant temperature change.	3.1(1h)A	3.1(2g)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvb79455	The critical fault code F1000227 no longer occurs on both the primary and subordinate FI during upgrade.	3.1(1e)A	3.1(2g)A
CSCvc02297	The power cap application no longer fails for a Bladeserver when the server is powered on or off from outside of Cisco UCS Manager.	3.1(1e)A	3.1(2g)A
CSCvc05615	FI-6396UP with FC 16G interfaces (individual/port-channel) no longer incorrectly report discard frame count. The issue was a cosmetic one where-in the discard count (both input and output) used to increase every few minutes. The interfaces themselves are not impacted and remain up.	3.1(1e)A	3.1(2g)A
CSCvd05543	For Cisco B460 M4 and B260 M4 Blade servers, a change to the PWRSEQ_FAULT_N logic from PWRSEQ_WARN_N to Pwr fault no longer results in a discovery failure if the master and slave blades have different board controller versions.	3.1(2f)B	3.1(2g)B
CSCvd20170	A Cisco UCS Manager power group change implemented through the HTML5 GUI no longer shows 0W for a Bladeserver in the chassis.	3.0(2c)A	3.1(2g)A
CSCvd42163	During a Fabric Interconnect upgrade or reload, the following error no longer occurs. `ERROR: bootflash: has unrecoverable error; please do "format bootflash:"`	3.1(1e)A	3.1(2g)A

Resolved Caveats in Release 3.1(2f)

The following caveats are resolved in Release 3.1(2f):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCva14937	M4 blades installed with SD cards instead of a hard disk no longer halt at 'Local Drive' for automated deployments with the following boot policy: Boot Policy • CD/DVD • Local Drive • Network Adapter (PXE)	2.2(3f)B	3.1(2f)B
CSCva35757	Latency between the UCS Manager Client and fabric interconnect no longer causes the firmware page to load slowly.	2.2(7b)A	3.1(2f)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvb52847	On a B200 M4 blade platform, instead of a NVMe plane, if RAID card is plugged in, then the /var/log/messages file no longer shows "Mux write error" messages. Apart from /var/log/message flood, no functional impact to normal storage operations are noticed.	3.1(2b)B	3.1(2f)B 3.1(3a)B
CSCvb63893	In a Cisco UCS Manager managed environment, the disk inventory is now able to refresh all the disks present on the system after a power cycle.	3.1(2b)C	3.1(2f)C
CSCvb69390	The value of "Input Discards" now only counts the value of snmpIfInDiscards from the HW counter.	3.1(2b)A	3.1(2f)A
CSCvb85331	The following fault no longer occurs after a UCS Manager software upgrade. Code: F1781 Description: Management database version mismatch detected failover may not complete Affected Object: sys/mgmt-entity-B Name: Mgmt Entity Mgmt Db Version Mismatch Cause: Replication Failure Type: Management	2.2(8c)A	3.1(2f)A
CSCvc03033, CSCvc31880, CSCvc06578, CSCvc85609	When all the UCS Blades are powered on at once, no server fails discovery with an insufficient power error.	3.1(2b)A	3.1(2f)A
CSCvc10791	A DME process no longer crashes when the dynamic vNIC and static vNIC contain a different adminVcon property value.	2.2(3e)A	3.1(2f)A
CSCvc26023	The Commvault backup application workload on the Cisco UCS-C3K-M4Raid Controller no longer hangs the system.	3.1(2e)B	3.1(2f)B
CSCvc14810	Systems with 6300 Fabric Interconnects and Windows Server 2012 virtual machines will no longer experience intermittent packet loss due to missing VLAN translate entries.	3.1(1e)A	3.1(2f)A
CSCvc29340	The Cisco UCS 2304 I/O Module no longer reboots and generates a kernel core due to a CPU soft lockup.	3.1(2c)A	3.1(2f)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvc31867	When upgrading the SSD to firmware 32F3Q, the firmware is no longer truncated and written as 2F3Q, which may cause a second request for the reboot of the server.	2.2(8a)A	3.1(2f)A
CSCvc39322	For B260 M4 Blades, BIOS v3.1.2.2 no longer intermittently fails Windows HLK and HCK Trusted Platform Module (TPM) tests on Windows Server 2016 and Windows Server 2012 R2.	2.2(7b)B	3.1(2f)B
CSCvc46313	The remote operation of making the LUN online from UCS Central no longer fails with the error message: `Global Service profile [org-root/org-GKDC/org-<name>/ls-SP_3260_03] can not be modified from UCS domain. Please make the changes from UCS Central that you are registered with.`	2.2(4b)A	3.1(2f)A
CSCvc60876	The 6248, 6296, and 6332 Series Fabric Interconnects no longer sends Smart Call Home messages in the wrong format.	2.2(8b)A	3.1(2f)A
CSCvc89242	The Fabric Interconnect no longer reboots due to a CDP process crash.	2.2(6e)A	3.1(2f)A
CSCvc95647	UCS Manager no longer incorrectly reports the following low memory warning on blade servers with KVM mounted scriptable vMedia: `F1704 275625 sys/chassis-x/blade-y/mgmt/health Health Warning <date> CimcLowMem : Please check the Health tab for more details`	3.1(2c)B	3.1(2f)B
CSCvd24330	IOM backplane down call home alerts (F1797) are no longer triggered when a blade is rebooted or shut down.	3.1(2b)A	3.1(2f)A
CSCvd27824	Storage controller and third-party adapter firmware update no longer fail, enabling the vNIC/HBA creation to proceed during a service profile association.	3.1(2e)A	3.1(2f)A
CSCvd12893	Servers no longer go into a pending reboot state each time a server disassociation/association or a decommission/recommission is performed.	3.1(2e)A	3.1(2f)A

Resolved Caveats in Release 3.1(2c)

The following caveats are resolved in Release 3.1(2c):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCux11611	Seagate hard drives left spinning idle without an operating system installed or setup with the JBOD configuration without read or write activity are no longer prone to failure. Impacted hard drives are listed here: • UCS-HD4T7KS3-E • UCSC-C3X60-HD4TB (4TB) • UCS-HDD3TI2F214 (3TB) • UCS-HDD2TI2F213 (2TB) • UCS-HDD1TI2F212 (1TB) • UCS-HD6T7KL4K • UCSC-C3X60-HD6TB • UCSC-C3X60-6TBRR	2.2(7c)B	3.1(2c)B

Resolved Caveats in Release 3.1(2b)

The following caveats are resolved in Release 3.1(2b):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCuy79306	When Cisco UCS C-Series servers with VIC 1225 or VIC 1227 are directly connected to Cisco Nexus 9000 switches, ports no longer go down or flap.	2.2(3f)C	3.1(2b)C
CSCun07367	Under normal state of operation, the statsAG process used to crash and restart on the Fabric Interconnect. This was also observed in the Cisco UCS Mini firmware. This issue has been resolved.	2.1(3a)A	2.2(7b)A 3.1(1e)A 3.1(2b)A
CSCuy83737	When the chassis containing a 4S server is decommissioned and then later is decommissioned with a different chassis number, the 4S server no longer goes into a mistmatched state instead of into discovery.	2.2(8a)A	3.1(2b)A
CSCuw19082	During Cisco UCS Manager initial setup, while configuring the fabric interconnect, setup will assume the GUI configuration method if a DHCP lease is obtained for the mgmt interface. In addition, an url will be provided for the setup of the fabric interconnect	2.2(6a)A	3.1(2b)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCuy52691	After upgrading Cisco UCS Manager, changes to the maximum power allocated will no longer prevent the blade server from powering on, with the following faults: **Description: Insufficient power available to power-on server x/y** **Affected Object: sys/chassis-x/blade-y/budget** **Name: Power Budget Power Budget Unavailable** **Description: [FSM:STAGE:RETRY:]: Check if power can be allocated to server x/y(FSM-STAGE:sam:dme:** **ComputeBladeDiscover:CheckPowerAvailability)** **Affected Object: sys/chassis-x/blade-yName: Fsm Sam Dme Compute Blade Discover** **Cause: Check Power Availability Failed**	3.1(1e)A	3.1(2b)A
CSCus03683	The Cisco UCS 6200 series primary and subordinate FIs no longer reboot unexpectedly due to high volume traffic impacting the management interface	2.2(1d)A	3.1(2b)A
CSCuw62466	In Cisco UCS Manager, Release 3.1, the new inband feature no longer causes failure in Cisco IMC failover detection when you connect multiple chassis	3.1(1e)A	3.1(2b)A
CSCva27558	In scenarios such as traffic loops in external networks, a series of MAC add or delete operations no longer causes the MAC address to display in the software table, and nor in the hardware table for all the ASICs.	2.2(5c)A	3.1(2b)A
CSCva61701	When the Cisco UCS FI uplinks are in the individual (" I ") state, broadcast traffic received on one interface is no longer sent back upstream on the other interfaces.	3.1(1e)A	3.1(2b)A
CSCva96740	Changes in adapter policy from UCS Manager now triggers a server redeploy.	2.2(8b)A	3.1(2b)A
CSCuu24614	FC port channel no longer gets deleted when Cisco UCS Manager perceives a speed difference between the port and port channel.	3.1(1e)A	3.1(2b)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCva04106	Removing a SAN port channel member no longer makes SAN ports to go down.	2.2(3d)A	3.1(2b)A
CSCuy98678	Cisco UCS 6296 fabric interconnect no longer crashes unexpectedly with kernel panic, and impact any devices connected the fabric interconnect.	2.2(6c)A	3.1(2b)A
CSCuz91263	A vulnerability in the command-line interface (CLI) of the Cisco UCS Manager and UCS 6200 Series Fabric Interconnects is resolved.	2.2(1a)A	3.1(2b)A
CSCuh73875	SNMP polling against FI drivers will no longer cause high volume of CPU usuage.	2.1(1a)A	3.1(2b)A
CSCus83447	Cisco UCS FI reload or switch over no longer occurs due to Leap second update.	2.2(1b)A	3.1(2b)A
CSCuw44595	DIMMs with correctable ECC errors are marked Inoperable or Degraded even though correctable errors do not affect normal system operation. This issue is now resolved.	3.1(1e)A	3.1(2b)A
CSCux03896	Cisco UCS Manager responds with a request timeout error to the client while requesting to associate servers, even if the request proceeds and is processed by the system. This leads to script timeouts or misleading GUI error messages. A new configurable field "Request Timeout" is introduced under the HTTP section of the GUI and CLI. User can increase the timeout that is configured in the http process so that an error is not returned to the client prematurely. This allows the request to wait for a longer time for a response from the system before returning an error.	3.1(1e)A	3.1(2b)A
CSCuy20188	When a fabric interconnect (FI) changes between switch mode and end-host mode, FI-A and FI-B no longer reboot together. The secondary FI reboots first. The primary FI waits for the secondary FI to come up and then reboots.	3.1(1e)A	3.1(2b)A
CSCuy81688	From Cisco UCS Manager tech-support, running /var/sysmgr/sam_logs/httpd_cimc.log on the affected fabric interconnect no longer shows the "exceeded max time without restart" error. From Cisco UCS Manager tech-support, running /ls_l.out on the affected fabric interconnect no longer shows the existence of a 'cimcrestart' file under /isan/apache/conf/. The modified date is now updated.	2.2(8a)A	3.1(2b)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCva47085	Cisco UCS Manager Release 3.1(2) addresses a link issue with UCS blade chassis infrastructure (633x FI and 2304 IOM) operating at 40G. Customers are recommended to upgrade to 3.1(2) if their deployment includes blade servers running at 40G.	3.1(1e)A	3.1(2b)A
CSCva73387	The SNMP process no longer crashes and causes the fabric interconnects to reload when DNS is configured on the fabric interconnects and SNMP trap hosts are configured with domain names.	3.1(1e)A	3.1(2b)A
CSCvb05762	UCS Manager GUI and CLI no longer fail to respond when the Data Management Engine (DME) hangs with a WaitOnLimit log message.	2.2(7b)A	3.1(2b)A
CSCuu81757	The vulnerability in the Secure Shell (SSH) management interface of the Cisco Unified Computing System (UCS) 6100 and 6200 Series Fabric Interconnect Series switches, which could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) because a Fabric Interconnect (FI) interface would not boot up completely, or cause high CPU utilization, is now resolved.	2.2(3f)A	3.1(2b)A
CSCul97240	When a UCS rack server is present in a UCS setup, DHCP renewal occurs frequently and Error level syslog messages are continuously sent to the syslog server configured through Cisco UCS Manager. However, these are false alarms because they do not affect the system. Sample syslog message: `0555 2016 Dec 12 12:07:55 UCS-A-1-A %DAEMON-3-SYSTEM_MSG: uid lease 127.5.99.2 for client 2c:2e:10:10:10:10 is duplicate on 10.1.0.0/10 - dhcpd`	2.2(1a)A	3.1(2b)A
CSCuz65286	Cisco UCS Manager firmware upgrade failed with the following message "UCSM upgrade validation failed" when the default value for IO throttle count in the FC adapter policy had a value of 16. This issue is resolved. The default IO throttle count is now set to 256.	3.1(1e)A	3.1(2b)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCuy99348	After the subordinate FI is rebooted or undergoes system update, HA was not ready and communication with primary DME timed out with the following error messages: HA state on primary: HA DOWNGRADED HA not ready on peer Fabric Interconnect HA state on secondary: HA NOT READY No device connected to this Fabric Interconnect CLI command timeout: Software Error: Exception during execution: [Error: Timed out communicating with DME] This issue is now resolved.	2.1(1a)A	3.1(2b)A
CSCuq57142	In a port channel universe the following symptoms no longer occur: • A port channel ID may sometimes not be released after use. This could eventually lead to the universe of port channel IDs being empty, and no port channel IDs being available for use. • After an upgrade, power loss, FI reboot or failover, the empty port channel universe is incorrectly interpreted as a new installation, and repopulated. Thisleadsto duplicate port channel ID allocation when a server is attached to the FI, or when a server is re-acknowledged.	2.2(3a)A	3.1(2b)A
CSCuy93451	VLANs are now deleted from the vNICs if they are deleted from the vNIC template.	2.2(7b)A	3.1(2b)A
CSCuz64184	For a fabric interconnect, when you replace the SFP of one of the links of a port channel, the entire four link FC port channel between the fabric interconnect and MDS switch goes down. This issue is now resolved.	2.2(6d)A	3.1(2b)A
CSCux07578	Cisco UCS Blade servers B400 M1 or B400 M2 that run on Liberator firmware version 4.10 with SATA drives no longer experience data consistency failures.	3.1(1e)B	3.1(2b)B

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCux21413	When you remove and reinsert a drive in the same slot, the Locator Storage Locator LED no longer remains solid ON.	3.1(1e)B	3.1(2b)B
CSCvs34343	When using Cisco UCS blade servers B200 M4 the PVOV75_STBY no longer throws an alert.	2.2(6e)B	3.1(2b)A
CSCuy13596	During OS installation on Cisco UCS C3260 System running Cisco VIC firmware 4.1(1d) and CMC firmware 2.0(9d), the installer no longer fails when creating partitions or writing to LUNs.	3.1(1e)B	3.1(2b) A

Resolved Caveats in Release 3.1(1l)

The following caveats are resolved in Release 3.1(1l) :

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvb90616	Fabric Interconnect no longer crashes during an image upgrade due to memory corruption with the following error: `SMI: System watchdog timed out`	3.1(1g)A	3.1(1l)A
CSCuu99255	The "show fabric-interconnect inventory expand " command no longer displays the ethernet port with a role of “Unknown” instead of "Server".	2.1(1a)A	3.1(1l)A
CSCuw50361	While collecting IOM tech-support by using the command "show platform software satctrl global", the HIF/NIF interfaces of an IOM no longer flap due to SDP heartbeat timeout.	2.2(4b)A	3.1(1l)A
CSCuy52691	After upgrading to Cisco UCS Manager Release 3.1(1e), the blade server no longer fails to power on with the following faults: Description: Insufficient power available to power-on server x/y Affected Object: sys/chassis-x/blade-y/budget Name: Power Budget Power Budget Unavailable	3.1(1e)A	3.1(1l)A
CSCva71801	UCS Manager no longer fails to synchronize with the IPv6 NTP server.	2.2(8a)A	3.1(1l)A
CSCvb78971	When attempting the auto-install of UCS Manager, the fabric interconnect upgrade no longer fails when the /var/tmp usage exceeds 10%.	2.2(3k)A 3.1(1e)A	3.1(1l)A
CSCvb82862	EUI-64 bit addresses can now be entered for storage connection policies or SAN boot targets.	2.2(8d)A	3.1(1l)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvb85544	A race condition in the Linux kernel's memory subsystem that handled the copy-on-write (COW) of read-only memory mappings no longer occurs on fabric interconnects. This bug has been filed by PSIRT against the product Cisco UCS Manager and Cisco UCS 6200 Series Fabric Interconnects to address the vulnerability known as "Linux Kernel Local Privilege Escalation (Dirty CoW)" and identified by CVE: CVE-2016-5195	2.2(1a)A	3.1(1l)A
CSCvb90517	Both fabric interconnects no longer reboot with vim hap reset reason codes.	3.1(1g)A	3.1(1l)A
CSCvc17769	The fabric interconnect no longer crashes when the bound interface of a Veth is in the "Not Initialized State" during a VLAN configuration change.	2.2(7c)A	3.1(1l)A
CSCuy81688	From Cisco UCS Manager tech-support, running /var/sysmgr/sam_logs/httpd_cimc.log on the affected fabric interconnect no longer shows the "exceeded max time without restart" error. From Cisco UCS Manager tech-support, running /ls_l.out on the affected fabric interconnect no longer shows the existence of a 'cimcrestart' file under /isan/apache/conf/. The modified date is now updated.	2.2(8a)A	3.1(1l)A
CSCvb18143	ACL Fabric Manager core is no longer seen during Cisco UCS Manager upgrade or downgrade to 3.1(1l) or higher.	2.2(8c)A	3.1(1l)A
CSCuz53730	Under heavy load on httpd, either from API, Cisco UCS Central and/or Cisco UCS Manager sessions, Cisco UCS Manager httpd process will no longer experience high memory usage or crash with a core file showing indications of memory allocation failure.	2.2(2c)A	3.1(1l)A
CSCul97240	When a UCS rack server is present in a UCS setup, DHCP renewal now triggers Information level syslog messages to be sent to the syslog server configured on Cisco UCS Manager.	2.2(1a)A	3.1(1l)A
CSCva56277	During downgrade of Cisco UCS Manager A bundle, the slots 3 and 4 in the fabric interconnect are no longer reported as powered off.	2.2(3a)A	3.1(1l)A
CSCva85907	During discovery of Cisco UCS C240 M4 server with Intel x520, Emulex 11102, and Qlogic 844 converged network adapters, the Intel X520 adapter no longer reverts to old firmware after a successful host firmware package (HFP) update.	3.1(1e)A	3.1(1l)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCva38476	An infrastructure software upgrade to UCS Manager 2.2(7b) or higher no longer fails when both fabric interconnects are incompatible or when one of the fabric interconnects is unresponsive.	2.2(7b)A	3.1(1l)A
CSCva34343	Cisco UCS Manager no longer reports false alerts due to P0V75_STBY sensor in Cisco B200 and M4 Blade Servers.	2.2(6e)B	3.1(1l)B
CSCuz21644	When Internet Explorer 11 browser is used to download the license file through Cisco UCS Manager **Admin** > **License Management** > **Download tasks** > **Download license file** > **Local File System**, the local file system no longer fails.	3.1(1e)A	3.1(1l)A
CSCva36811	When logging into Cisco UCS Manager through HTML5, if a password length greater than 32 characters is configured, it results in the following authentication error: `Login Error: Authentication failed` This issue is now resolved.	3.1(1g)A	3.1(1l)A
CSCva27558	In scenarios such as traffic loops in external networks, a series of MAC add or delete operations no longer causes the MAC address to display in the software table, and nor in the hardware table for all the ASICs.	2.2(5c)A	3.1(1l)A
CSCva61701	When the Cisco UCS fabric interconnect uplinks are in the individual (" I ") state, broadcast traffic received on one interface is no longer sent back upstream on the other interfaces.	3.1(1e)A	3.1(1l)A
CSCvb08928	Cisco UCS fabric interconnect no longer reboots when VLAN is deleted.	2.2(5a)A	3.1(1l)A
CSCva73387	The SNMP process no longer crashes and causes the fabric interconnects to reload when DNS is configured on the fabric interconnects and SNMP trap hosts are configured with domain names.	3.1(1e)A	3.1(1l)A

Resolved Caveats in Release 3.1(1k)

The following caveats are resolved in Release 3.1(1k):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCuu40291	When debug logging is enabled, Cisco UCS Manager tech-support showed that syslogd_debug files were present, but the `show debug logfile syslogd_debugs` CLI command failed with the following error: `Logfile(syslogd_debugs)does not exist` This issue is now resolved.	2.2(3a)A	3.1(1k)A
CSCuu40978	The syslog is now truncated after it reaches the configured maximum size. It no longer fills up the Fabric Interconnect file system.	2.2(3d)A	3.1(1k)A
CSCuv45574	After downgrading the controller firmware on C220/C240 M3 systems with LSI 9271-8i controller, the GUID of virtual disks no longer change and the virtual machines running on the ESXi OS no longer become inaccessible.	2.2(6f)A	3.1(1k)A
CSCux38896	UCS Mini FC ports in F mode will no longer be stuck in "init" state after a reboot of the fabric interconnect.	3.0(2d)A	3.1(1k)A
CSCux53224	A fatal error is no longer observed when creating or removing virtual drives with RAID 5 and RAID 6 controller combination.	3.1(1g)C	3.1(1k)C
CSCux62816	When any IPMI user attribute is modified, it will not block authentication for the IPMI user and all the related operations that need authentication. User is able to login, inject UC ECC error, or perform IPMI related operations with the IPMI tool.	3.1(1e)A	3.1(1k)A
CSCux73294	Server discovery is no longer stuck with the following error message: `AssociateNicUnconfigPnuOSLocal failure Adapter: repo lookup failed` This was seen in the server discovery sequence, whenever the static adapter MAC address on VLAN 4043 got deleted in the hardware table.	2.2(6b)B	3.1(1k)B

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCux96072	During heavy I/O traffic, the Cisco 12G Modular RAID controller no longer goes offline with the "`Storage Controller SLOT HBA inoperable`" error logged in Cisco IMC event logs.	2.2(6e)B	3.1(1k)B
CSCuy35745	When upgrading or downgrading a Unified Ports Capable 3rd Generation Fabric Interconnect, the upgrade or downgrade process no longer fails with the following error message: `less space in /var/sysmgr`	3.1(1e)A	3.1(1k)A
CSCuz54661	Cisco B200 M3 Server no longer fails to post if NUMA is disabled.	2.2(7b)B	3.1(1k)B
CSCuz08759	vniccfgd process no longer crashes when downgrading VIC firmware to version 4.1(1d).	3.1(1e)B	3.1(1k)B
CSCuz86450	The server no longer reboots because the system does not accept user input on the order property of adaptorHostIf.	1.4(1j)A	3.1(1k)A
CSCuz92668	Vulnerabilities affecting various versions of NTPd are now resolved.	2.2(1a)A	3.1(1k)A
CSCuz97205	The server no longer reboots when any trivial change is made on the service profile, as Cisco UCS Central does not push a purpose property change on the VLAN under vNIC.	3.1(1g)A	3.1(1k)A
CSCva08256	Cisco IMC and BIOS no longer get stuck updating or activating with the host firmware pack when the new host firmware pack has the same name and version as the system being updated.	2.2(7b)A	3.1(1k)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCva09070	When opening the following Cisco UCS Manager pages in an Iframe, the Cisco UCS Manager URL will open in a new tab instead of an Iframe, thus preventing the click-jacking issue. Here the issue of click-jacking has been fixed using Frame Breaking Script instead of using X-Frame-Options header, because though the X-Frame-Options header is supported by all the major browsers, it is not standardized. Also, differences exists with respect to the implementation details between different browsers. Please refer the following link for further details https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet The following Cisco UCS Manager pages do not use an X-Frame-Options response header : • https://xx.xxx.xxx.x/app/3_1_1e/ • https://xx.xxx.xxx.x/ • https://xx.xxx.xxx.x/cgi-bin/main.cgi • https://xx.xxx.xxx.x/ucsm/kvm.html • https://xx.xxx.xxx.x/app/3_1_1e/index.html • https://xx.xxx.xxx.x/app/3_1_1e/kvmlauncher.html	3.1(1e)A	3.1(1k)A
CSCva01733	PXE in Legacy Boot mode no longer hangs with excessive unicast or multicast high background traffic with a packet size larger than MTU directed to the client server. This was seen with ESXi Autodeploy on a specific setup which likely had unusually high multicast traffic directed at the client server. This traffic was not from the PXE server for file transfer, but from some other source.	2.2(6e)B	3.1(1k)B

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCva19523	When the Peer Fabric Interconnect is down, the server discovery FSM is no longer stuck with the following message: `"detect mezz cards in 1/1(FSM-STAGE:sam:dme:ComputeBlade Discover: NicPresencePeer)"` **Note** This no longer happens with other FSMs as well, with the same condition of the Peer Fabric Interconnect being down.	3.1(1e)A	3.1(1k)A
CSCva29365	Enabling stateless offloads for NVGRE in the following 3rd generation Cisco VIC adapters' configuration with Cisco UCS Manager/Cisco IMC no longer leads to inaccessible vNIC interfaces in the host OS: • UCSC-C3260-SIOC • UCSB-VIC-M83-8P • UCSB-MLOM-40G-02 • UCSB-MLOM-40G-03 • UCSC-PCIE-C40Q-03 • UCSC-MLOM-C40Q-03	2.2(7a)B	3.1(1k)B
CSCva34426	Cisco UCS 3X60 Server no longer fails to boot from LSI RAID controller managed disk slots 1 or 2, when the disks are in JBOD mode	2.2(7c)A	3.1(1k)A
CSCva54957	A reboot is no longer triggered without a “user-ack” when modifying a service profile that requires a reboot while shallow association is failing.	2.1(3a)A	3.1(1k)A
CSCva72096	Cisco UCS servers running Intel E5 Xeon v4 CPUs no longer crash with a signature pointing to internal parity errors, page fault, general detect, or undefined opcode exceptions.	2.2(4b)B	3.1(1k)B

Resolved Caveats in Release 3.1(1h)

The following caveats are resolved in Release 3.1(1h):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCuj71400	Cisco UCS Manager no longer displays the “FCoE or FC uplink is down on VSAN X” fault when the member ports for the VSAN are up.	2.2(1a)A	3.1(1h)A
CSCuq74472	Unnecessary thermal events on IOM stating "Thermal sensor reading not available" no longer occur.	2.1(3c)A	3.1(1h)A
CSCux58865	DIMM temperature readings are no longer missed when the temperature is 10 degrees Centigrade more than the previous reading.	2.1(3d)B	3.1(1h)B
CSCuy62783	In a UCS setup with a VIC13xx adapter on blade servers or rack-mount servers, the server or VIC adapter no longer becomes unresponsive after running IO across network file systems.	2.2(3a)B	3.1(1h)B
CSCuy64856	The Cisco UCS fabric interconnects (FI) are no longer rebooted due to fwm hap reset.	2.1(3h)A	3.1(1h)A
CSCuz46574	After a VM changes its pinning, the MAC address of that VM is now removed immediately from the MAC address table of the Cisco UCS 6332 FI to which it was earlier pinned.	3.1(1e)A	3.1(1h)A
CSCuz69373	During Cisco UCS Manager upgrade to release 3.1(1), you will no longer see CATERR faults due to unresponsive eCPUs. This issue happens when the eCPUs fall into diagnostic code (debug loop) after the DINT CPU input is asserted.	3.1(1e)A	3.1(1h)A
CSCuy01645	DIMM temperature readings are no longer missed when the temperature is 16 degrees Centigrade more than the previous reading.	3.1(1e)B	3.1(1h)B

Resolved Caveats in Release 3.1(1g)

The following caveats are resolved in Release 3.1(1g):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCuz46609	You will see inconsistent behavior with Driver Locator LEDs in the following scenarios: • The board controller package for Cisco UCS B200 M4 blade servers is version 12 and the storage controller/adapter firmware version is not running on the latest version. • The board controller package for Cisco UCS B420 M4 blade servers is version 6 and the storage controller/adapter firmware version is not running on the latest version. This issue is no longer seen if the board controller packages and the storage controller/adapter firmware version meet the requirements in the system specification.	3.1(1e)B	2.2(7b)B, 3.1(1g)
CSCuv46749	When using Cisco B200 M4 blade servers with the UCSB-MRAID12G storage controller, the following random, incorrect transient alerts or faults are no longer reported: • Critical Fault [F1004] Controller Inoperable, Reason: Device reported corrupt data. • Critical Fault [F1004] Controller Inoperable, Reason: Device non-responsive.	2.2(3g)A, 2.2(6d)C, 3.0(2c)B	2.2(6f)B, 3.1(1g)
CSCuv89839	When the fabric interconnect is in switch mode with direct attached storage, and its FC uplinks to the direct attached storage are up, these FC uplinks now allow traffic to pass.	2.2(3f)A	2.2(6g), 3.1(1g)
CSCuv97713	After upgrading Cisco UCS Manager, in rare cases, the IOM may core in the sysmgr process leading to IOM reboot. This is now resolved.	2.2(3j)A	2.2(6g)A,3.1(1g)
CSCux05389	After upgrading to release 2.2(7a) and rebooting the subordinate fabric interconnect, occasional VSAN misconfiguration will no longer occur.	2.2(6g)A	3.1(1g)A
CSCux39987	DME communication outage will no longer be seen when policy ownership is validated.	2.2(6g)A	3.1(1g) A
CSCux66675	After rebooting a Cisco UCS 6296UP FI, all physical interfaces will no longer connect incorrectly with the Cisco UCS C460 M4 servers.	2.2(6c)A	3.1(1g)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCux68195	VMware ESXi crash (Purple Screen of Death) will no longer be seen during certain operations while running VM FEX.	3.1(1e)A	3.1(1g)A
CSCux68679	When a UCS B460 M4 server is configured with Fusion IO cards installed in same mezzanine slot of the master and slave blades, actions such as Cisco UCS Manager upgrade, cluster failover, fabric interconnect reboot no longer trigger server reboot.	2.2(3a)A	2.2(6g)A, 3.1(1g)A
CSCux85580	Fabric Interconnect cores will no longer be seen on IGMP.	2.2(3b)A	3.1(1g)A
CSCuy07652	During downgrade or upgrade of Cisco UCS Manager from release version 2.2(6c) to 2.1(3g), UCSM GUI is no longer stuck in the "registering" state.	2.2(6g)A	3.1(1g)A
CSCuy25170	On Cisco UCS Mini or Cisco UCS 6300 Series Fabric Interconnects with Dual Voltage PSUs, incorrect PSU status will no longer be displayed for two fields: PSU wattage and PSU type.	3.1(1e)A	3.1(1g)A
CSCuy60819	When upgrading Cisco UCS Manager build or rebooting the primary FI, a rediscovery/association for the Cisco UCS B460 M4 server that includes third generation Fusion IO will no longer be triggered.	2.2(6a)A	3.1(1g)A
CSCux65310	During blade discovery or Cisco IMC controller reset, a chassis thermal critical fault can be generated due to the time it takes for reconnecting from the IOM to the Cisco IMC. However, after several minutes this fault clears on its own.	3.1(1c)A	3.1(1g)A
CSCuw36128	During normal Cisco UCS Manager operation, the following equipment fault will no longer be seen for an extended period of time: `Major Fault "F0885: Fabric Interconnect B inventory is not complete [illegible] seen.`	3.0(2c)A	3.1(1g)A
CSCuy48772	Cisco UCS Manager will no longer allow the regeneration of a self-signed default certificate without a valid key size.	3.1(1e)A	3.1(1g)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCux70856	The following symptoms will no longer be seen after rebooting the primary FI or UCSM cluster failover: 1. Appliance port down on the FIs 2. Network control policy named 'default' automatically changes from 'Warning' to 'Link down' for the 'Action on Uplink fail' property.	2.2(3g)A	3.1(1g)A
CSCuw55142	Cisco UCS B420M4 server with the UCSB-MRAID12G-HE no longer reports the following critical fault: `"Controller 1 on server is inoperable. Reason: Device non-responsive"`	3.1(1e)B	3.1(1g)B
CSCuw46478	The Local disk Locator LED no longer remains OFF after it is enabled in Cisco UCS Manager.	3.1(1e)B	3.1(1g)B
CSCuv43349	During server discovery or during Cisco UCS Blade server association or disassociation, the following failures are no longer reported: • `Waiting for BIOS Post Completion` • `Unable to get SCSI Device Information from the system`	3.1(1e)B	3.1(1g)B
CSCuz74973	When you use a B200 M4 server with a UCSB-MRAID12G SAS RAID controller and a CPLD firmware version earlier than version 05D, the B200 M4 server no longer powers off unexpectedly.	3.1(1e)B	3.1(1g)B

Resolved Caveats in Release 3.1(1e)

The following caveats are resolved in Release 3.1(1e):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCug14669	A Fibre Channel (FC) path loss occurred because the Fibre Channel Forwarder (FCF) MAC address was learned dynamically. This issue is now resolved.	2.1(1b)A	3.1(1e)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCun07367	Under normal state of operation, the statsAG process used to crash and restart on the Fabric Interconnect. This was also observed in the Cisco UCS Mini firmware. This issue has been resolved.	2.1(3a)A	2.2(7b)A 3.1(1e)A 3.1(2b)A
CSCuh52458	Cisco UCS fabric interconnects go into a reboot cycle when a spanning tree loop is introduced on an uplink switch connected to a management port. This issue is now resolved.	2.1(1e)A	3.1(1e)A
CSCuo60528	Issues related to time Cisco IMC date/time sync in Cisco UCS Mini are resolved.	3.0(1c)	3.1(1e)A
CSCuo89748	Under rare conditions in a scale deployment, the Cisco UCS Manager GUI may crash with the following error message: `Fatal Error: Event sequencing is skewed, Would you like to login again or exit?` This issue is now resolved.	2.2(2a)A	3.1(1e)A
CSCus61298	When you have FEX and Chassis in your Cisco UCS environment it may cause Chassis Limit Exceeded error , although the total number of FEX and Chassis is less than twenty on each fabric interconnect. This issue is now resolved.	3.0(1c)	3.1(1e)A
CSCut60576	The buffer overflow condition that caused the blade AG process to crash and core is now fixed.	2.2(3b)A	3.1(1e)A
CSCut67768	Blade server discovery may fail with the error PciAddress of Storage Controller not found, when a Fusion IO card is present in the blade. This issue is now resolved.	3.0(1c)	3.1(1e)A
CSCuu30803	The Cisco UCS 6324 fabric interconnects with Cisco UCS Manager Release 3.0 versions and higher can enter a state where the tftpd service has been stopped, and not restarted. This can happen in the following scenarios: • Decommissioning or re-commissioning of a server • Association of a service profile with the local disk policy flexflash set to 'yes', and default boot policy enabled This issue is now resolved.	3.0(2c)B	3.1(1e)B

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCuw53461	A Fibre Channel (FC) port on a Cisco UCS 6324 fabric interconnect may go into the hwfailure state. This issue is now resolved	3.0(2d)A	3.1(1e)A
CSCux05630	Cisco UCS 6324 fabric interconnect may lose all connectivity due to MTS buffer leak with continuous port-flapping. This issue is now resolved.	3.0(2c)	3.1(1e)A
CSCui13596	In a Cisco UCS NX-OS CLI environment, when the command `show run vdc-all` is used few times, `snmp-server enable traps entity fru` will appear in a different location of the display. This issue is now resolved.	2.1(2a)A	3.1(1e)A
CSCuq75690	Cisco UCS Manager displays show operation patrol read failed error although SSD's are present in the system. This issue is now resolved.	2.2(3e)A, 2.2(2c)A	3.1(1e)A
CSCus22311	The Show Logging Log will not contain Virtual Ethernet Bridge Protocol Data Unit (vEth BPDU) related error information. You can use show interface for the status of the vEth BPDU guard error.	2.2(3a)A	3.1(1e)A
CSCus45089	FlexFlash RAID Reporting State can now be set correctly in Cisco UCS Manager GUI during creation of Local Disk Configuration Policy.	2.2(3c)A	3.1(1e)A
CSCut10662	When a default VSAN port configured on a FC port is deleted, one of the following can occur: • The port remains in error_disabled state. • The default VSAN port changes to 1. This issue is now resolved.		3.1(1e)A
CSCut44138	In some cases, attempts to unconfigure an uplink interface on a fabric interconnect may fail on Cisco UCS Manager version 2.1(3h).	2.1(3b)A	3.1(1e)A
CSCuv15516	The Cisco UCS C240 M4 servers may not boot to LSI SW RAID disk after an upgrade to Cisco UCS Manager version 2.2(4b). This issue is now resolved.	2.2(3f)C	3.1(1e)C

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCuv19605	Cisco UCS B200 M4 servers with Cisco VIC 1340 Adapter may not set the host port for the vNICs after configuring the LAN or SAN connectivity policy. This issue is now resolved.	2.2(5a)A	3.1(e)A
CSCuv35387	Cisco UCS Mini core files generated by the dmserver process may not be decoded accurately. This issue is now resolved.	3.0(2c)A	3.1(1e)A
CSCut43020	When configuring IP pools, invalid IP addresses can be allocated by Cisco UCS Manager as part of the IP address range for the pool. This issue is now resolved.	2.2(3d)A, 2.2(2c)A	3.1(1e)A
CSCuu04780	Erroneous interrupts from the Chassis locator LED cause dmserver cores on the fabric interconnect. Thermal alerts are observed shortly before the core dump happens. This issue is now resolved.	3.0(2c)	3.1(1e)A

CSCuu53553	Installing the port license on Cisco UCS Manager will not fail with the following critical license error messages:
	`Error code: F0677: license-file-uninstallable.`
	`Error code: F1000091: [FSM:FAILED] : Installing license file B\port29.lic(FSM:sam:dme:LicenseFileInstall)`
	This issue is now resolved.
		2.2(3e)A	3.1(1e)A

CSCuu97312	For direct connected Cisco UCS C-Series Servers, the Cisco UCS Manager GUI will no longer show server port mode as Unknown instead of Fabric.	2.2(4b)A	3.1(1e)A
CSCuw62466	In Cisco UCS Manager, Release 3.1, the new inband feature causes failure in Cisco IMC failover detection when you connect multiple chassis. When you connect multiple chassis, the traffic is not isolated. So Cisco IMC takes local management traffic as valid route traffic and does not fail over.	2.2(3j)B	3.1(1e)B
CSCuv04248	In Cisco UCS Manager releases earlier than 3.1, in 6200 Fabric Interconnects, you could configure more than 2000 active vLANs. With release 3.1, you can only configure up to 2000 active vLANs in any platform.	3.1(1e)A	3.1(1e)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCuu62336	In Cisco UCS Manager releases earlier than 3.1, when you add an unsupported port to a port channel, the system let you submit the change, and then the action failed. With release 3.1, the system displays an error when you try to submit an unsupported port channel assignment.	3.1(1e)A	3.1(1e)A
CSCuv66933	When you perform upgrade from Cisco UCS Manager, release 3.0 to 3.1, if you have SNMPwalk running, snmpd crashes.	3.1(1e)A	3.1(1e)A
CSCux12266	The Cisco UCS Blade server B200 M3 FSM remains stuck in the "Discover PnuOS Inventory" stage. Also, the KVM console remains stuck at the "PnuOS" prompt in the following scenarios: • Blade discovery. • Any condition that causes Target Boot ID corruption.	3.1(1e)B	3.1(1e)B
CSCux07578	If you have Cisco UCS Blade servers B400 M1 or B400 M2 running on Liberator firmware version 4.10 with SATA drives, you may see data consistency failures.	2.2(7b)B	3.1(1e)B
CSCux21413	When you remove and reinsert a drive in the same slot, the Locator Storage Locator LED remains solid ON.	2.2(6b)B	3.1(1e)B
CSCuv46749	If you have Cisco UCS Blade servers B200 M4, B420 M4, B260 M4, B460 M4 in your environment, you will see random, transient alerts in the controller reports. **Note** This issue is seen as part of statistics/reporting and not in the actual system	2.2(3g)A	3.1(1e)A
CSCuw55142	Cisco UCS B420M4 server with the UCSB-MRAID12G-HE may report the following critical fault: `"Controller 1 on server is inoperable. Reason: Device non-responsive"`	2.2(6f)B	3.1(1e)B
CSCuw46478	The Local disk Locator LED remains OFF, although enabled in Cisco UCS Manager.	2.2(7b)B	3.1(1e)B

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCuy46062	When downloading a technical support file, you will not be able to specify the path where the file can be downloaded .	3.1(1e)B	3.1(1e)B

Open Caveats

The open bugs for a release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains up-to-date information about bugs and vulnerabilities in this product and other Cisco hardware and software products.

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

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

Open Caveats for Release 3.1(3h)

The following caveats are open in Release 3.1(3h):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvk71319	The message queue may become full and if the VIM misses a heartbeat can result in VIM process crash.	There is no known workaround.	3.1(3h)A Resolved in 3.1(3k)A
CSCvj10772	Multicast traffic may drop on some Veths. The affected multicast group(s) are seen in the software but absent in the hardware.	Disable then enable the IP IGMP snooping on the affected VLAN or globally.	3.1(3h)A Resolved in 3.1(3k)A
CSCvk51589 CSCvk73712 CSCvk75400	Cisco UCS 6200 and 6300 Series Fabric Interconnects may reload with the message: Reset triggered due to HA policy of Reset. This error may occur if the message queue becomes full.	There is no known workaround.	3.1(3h)A Resolved in 3.1(3k)A
CSCvi98058	New OS installation in UEFI mode and BIOS version 2.2.6f.0 fails.	Install the OS using an earlier version of BIOS, for example 2.2.6e.0 and then upgrade to 2.2.6f.0 version.	3.1(3h)B Resolved in 3.1(3j)

Open Caveats for Release 3.1(3e)

The following caveats are open in Release 3.1(3e):

Defect ID	Symptom	Workaround	First Bundle Affected

CSCvh56396	mgmt0 IP may not appear in the command "show ip interface brief vrf management" or "show run interface mgmt0" from connect nxos.	Change the IP address of the affected fabric interconnect through the UCSM GUI or CLI to a different IP and then change the IP back to the original IP.
		Alternatively, engage TAC to update mgmt0 IP or a reboot of the FI may also resolve the issue.
		If CSCve06658 is a concern, then prior to the upgrade or reload, shutdown the Ethernet uplinks to ACI before the FI reloads.
		Verify that mgmt0 IP is assigned using:
		`connect nx a/b`
		`show ip interface brief vrf management`
			3.1(3e)A
			Resolved in 3.1(3f)A

Open Caveats for Release 3.1(3d)

The following caveats are open in Release 3.1(3d):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvh07966	A firmware update may fail for Nvidia P100.	Use the native OS utility tools to manually update the firmware for the P100 board.	3.1(3d)C Resolved in 3.1(3f)C
CSCvg88563	Both sockets of the Rack Server with UCSC-GPU-M60 may not display the same firmware version.	Workaround to match both processors with the same firmware version can be made using native OS based tools to manually upgrade the firmware on both the processors.	3.1(3d)A Resolved in 3.1(3f)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvh04298	The IOMs connected to an FI reboot unexpectedly due to a software-controlled reset.	There is no known workaround for this issue. Enable fabric failover/ NIC teaming for critical servers, so that there is no traffic loss.	3.1(3d)A Resolved in 3.2(3a)A

CSCvg28969	The following NVMe drive PID may not appear correctly for Cisco UCS S3260 Storage Servers when viewed through the HTML5 GUI.
	Incorrect PID
	• UCSC-NVMEHW-H800
	• UCSC-NVMEHW-H1600
	• UCSC-NVMEHW-H6400
	Correct PID
	• UCS-S3260-NVM48
	• UCS-S3260-NVM416
	• UCS-S3260-NVM432
		Use the following CLI commands to verify the PID for NVMe drives.
		`scope chassis <Chassis ID>`
		`scope server <Server ID>`
		`scope raid controller <Raid Controller ID>`
		`NVME`
		`show detail expand`
		Look for the PID in the displayed list.
			3.1(3d)A

Open Caveats for Release 3.1(3c)

The following caveats are open in Release 3.1(3c):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvg21234	The Matrox display driver now loads correctly and works successfully on all M4 EP blade servers with Windows Server 2016.	There is no known workaround for this issue.	3.1(3c)B Resolved in 3.2(3a)B

Defect ID	Symptom	Workaround	First Bundle Affected

CSCvg64592	Rack servers integrated with UCS 6200 Series FIs, 6300 Series FIs and 6324 FIs do not have connectivity after reboot of the subordinate FI, if the VLAN range (expressed as a string of characters) applied on a port-profile exceeds 255 characters.
	Example: This issue will occur if the VLAN range is defined as the following:
	`switchport trunk allowed vlan24,58,301,1028,1029,1247,1718,1719, 1794,1795,1807,1818,2000,2001,2004,2009,2010,2066,2068,2069,2070,2078,2080, 2082,2084,2085,2086,2096,2097,2112,2118,2119,2794,2796,2941,3000,3001,3004, 3009,3010,3023,3030,3066,3068,3069,3070,3078,3080,3082,3084,3085,3086`
	The following error message is observed in the Primary FI extVMmAG log file:
	`Error redirecting cmd to PPM, error: 42, ret: 1108082899`
	A similar fault is observed in the output of the Cisco UCS Manager show fault command.
	`Severity: Critical Code: F999590 Description: [FSM:FAILED]: VNIC profile configuration(FSM:sam:dme:VnicProfileSetDeploy). Remote-Invocation-Error: Error redirecting cmd to PPM, error: 42, ret: 1108082899 Affected Object: fabric/lan/profiles Name: Fsm Sam Dme Vnic Profile Set Deploy Fsm Fail`
		To regain connectivity, ensure that the subordinate FI is made primary by initiating cluster failover.
		To avoid re-occurrence of this issue, if system is not using any DVS integration feature but has enabled "VM" as an option in the "Target" field of the vNIC template, then this option can be cleared to delete the port-profiles.
			3.1(3c)A
			Resolved in 3.1(3j) and 3.2(3a)A

CSCve08388	An update may fail for the local disk firmware image.	There is no known workaround.	3.1(3c)A Resolved in 3.1(3f)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvi96785	On UCS 6332-16UP and 6332 fabric interconnects, the following file system output state is seen: `Filesystem state: clean with errors` The following errors may also be observed: • The dmesg output may have the following entry: `EXT3-fs warning: mounting fs with errors, running e2fsck is recommended` • Show logging nvram may have following log: `%KERN-2-SYSTEM_MSG: [9604349.199019] EXT3-fs error (device sda3): ext3_readdir: directory #4791141 contains a hole at offset 0 - kernel`	If this issue occurs, performing a file system check may help. To repair a file system, contact TAC.	3.1(3c)A Resolved in 3.1(3j)

Open Caveats for Release 3.1(3a)

The following caveats are open in Release 3.1(3a):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvh66141	When accessing KVM directly without first logging into UCS Manager, KVM may fail to launch if you are using non-native authentication.	Use native authentication to log in or use Java and not HTML 5 KVM console.	3.1(3a)B Resolved in 3.1(3k)B
CSCvh64120	DME may crash after an upgrade to 3.1(3) or 3.2(2).	Contact Cisco TAC. TAC will need to manually downgrade UCS Manager to a release without the enhancements found in CSCva64277 and CSCva30433. TAC will need to manually edit the configuration to remove the Netflow from the service profiles.	3.1(3a)A Resolved in 3.1(3f)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvf32853	Blade upgrades may fail to boot and get stuck at "Waiting for BIOS POST completion" during a firmware update for storage controllers.	Create two host firmware packages: Create a Host Firmware Package for your target version that Excludes "Storage Adapters". This is only possible in UCSM 2.2(7b) and later. In previous versions you will have to create an Advanced Host Firmware Package and select all components except the Storage Adapters. Create a second Host Firmware Package that ONLY includes the Storage Adapters and select the versions that you are looking to upgrade to. You can do this by Excluding all other components, or by making an Advanced Host Firmware Package. How to upgrade the servers: To upgrade the servers, first upgrade all the components EXCEPT the Storage Adapter. So we will use the first Host Firmware Package created. Update the RAID Controller by itself by selecting the second Host Firmware Package created. You can now assign the Service Profile back to the original Host Firmware Package. Since all components have been upgraded, no further changes will be made.	3.1(3a)B 2.2(8a)B
CSCvf36433	Matrox G200e driver installation may produce an error on Windows 2016.	There is no known workaround. A host power cycle will clear the condition.	3.1(3a)C Resolved in 3.1(3f)C
CSCvf50470	Cisco VIC adapter may display an Exchange Allocation Failure and WQ Errors with fibre channel traffic.	Use the default drivers included in Windows 2016.	3.1(3a)B Resolved in 3.1(3f)B

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvf07449	The firmware update for the LSI 9300-8e controller may not get updated during the initial firmware update but an error is not reported. This may cause the firmware version to be incorrectly set to the latest version even though the actual firmware on the controller is older.	Update the controller from standalone mode or by using any of the recommended host OS utilities.	3.1(3a)A Resolved in 3.1(3c)A
CSCvf18955	During clustering, if one FI runs Release 3.1(3) and the other FI runs any release earlier than Release 3.1(3), an error message indicating that the local "Admin" password is incorrect, or that the authentication mode of the working fabric is not set to "Local" is displayed.	If the online FI is running Release 3.1(3) and the new FI to be clustered is running a release earlier than Release 3.1(3), then the new FI must be upgraded in standalone mode before attempting to re-cluster. For FI Cisco UCS 6200 Series and 6332 FIs, this can be done by setting up the new FI in standalone mode and following upgrade procedures. For UCS Mini 6324, if there are no separate unused chassis available to host this FI for the upgrade, then this FI must be upgraded manually using UCS FI recovery steps to rebuild the Kickstart, System, and UCSM images to Release 3.1(3) while in the existing chassis. Contact Cisco TAC for assistance.	3.1(3a)A Resolved in 3.1(3c)A
CSCve41254	LUN creation may fail using Local Disk policy with RAID 60 mode in rack servers.	There is no known workaround.	3.1(3a)A Resolved in 3.1(3b)A
CSCve46288	UCS S3260 storage controller upgrade may fail for M3 servers when upgrading from 3.1(2f)C to 3.1(3a)C.	There is no known workaround.	3.1(3a)A Resolved in 3.1(3b)A
CSCve35785	The SNMP process may crash on UCS after an upgrade due to high memory usage.	Avoid SNMP polling of UCS Manager.	3.1(3a)A Resolved in 3.1(3c)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCve30332	UCS Manager may become unresponsive when a Service Profile is associated with a server.	There is no known workaround.	3.1(3a)A Resolved in 3.1(3b)A
CSCve15708	UCS domain registration may fail on UCS firmware when using the IPv6 address of UCS Central.	There is no known workaround.	3.1(3a)A Resolved in 3.1(3b)A
CSCve06789	A service profile creation may fail with the SAN connectivity policy using vHBA when it is created with a redundancy pair.	Both the vHBAs corresponding to a redundancy pair have to be created manually by selecting the respective vHBA templates.	3.1(3a)A Resolved in 3.1(3b)A
CSCve13711	When upgrading UCS Manager, the remote fabric interconnect may continuously reboot with a PCIe Device-Cisco Donner error.	There is no known workaround.	3.1(3a)A Resolved in 3.1(3b)A
CSCve14154	In a system with the Infrastructure bundle at Release 3.1(3) and the C-Bundle at Release 3.1(2), disk zoning configuration with 'shared' ownership of disks used on HBA controller UCSC-C3X60-HBA present in M3 server UCSC-C3X60-SVRNB, fails with the following FSM error during chassis profile association: `Zoning Error: Invalid parameters`	No known workaround. Upgrade the C-Bundle to Release 3.1(3) for 'shared' mode to work on UCSC-C3X60-HBA controllers.	3.1(3a)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvd39706	The vMedia performance of an HTML5 and Javascript-based KVM client is slower than the vMedia performance of a Java KVM client.	Use the Java KVM client. To launch the Java KVM client from Cisco UCS Manager or KVM Launch Manager: 1. Click the >> next to the KVM Console or Launch buttons. 2. In the dialog box that appears, check the **Launch Java KVM Console** checkbox. For KVM Direct, the **Launch Java KVM Console** checkbox appears directly on the web page.	3.1(3a)A
CSCvd90035	When a Cisco UCS S3260 M4 server is used with an IO Expander module, Cisco UCS Manager is unable to create more than 64 virtual drives from the RAID controller on the server and the RAID controller on the IO Expander module.	No known workaround	3.1(3a)A
CSCvd27202	When using the **format card** command or the **Format Card** button on Cisco UCS M4 and higher servers, the host OS will not see a valid format on the SD card when Cisco IMC format is used.	Format the SD card at the host OS.	3.1(3a)A
CSCvd51029	Firmware downgrade fails on Cisco UCS Manager-managed C220 M4, C240 M4 and C460 M4 servers with an Emulex 14102 CNA card.	Exclude the Emulex 14102 firmware from the C-bundle.	3.1(3a)C
CSCvd58463	While upgrading firmware on Cisco UCS Manager-managed C-Series servers with a Broadcom 57810 adapter, the finite state machine (FSM) may become unresponsive.	Exclude the Broadcom 57810 adapter firmware from the Host Firmware Package.	3.1(3a)C

Defect ID	Symptom	Workaround	First Bundle Affected
CSCve05221	On Cisco UCS S3260 servers that are managed by Cisco UCS Manager, server association of server node 2 fails while upgrading the firmware.	Reset Cisco IMC.	3.1(3a)C

CSCvf50470	Server loses FC connectivity with the datastore, and the following errors are displayed in the Tech Support files:
	• Adapter log with messages similar to these:
	`170717-14:32:50.253197 ecom.ecom_main ecom(8:1): failed to allocate exchange 1664 times`
	`170717-14:32:50.353191 ecom.ecom_main ecom(8:1): failed to allocate exchange 1663 times`
	• Host VMWARE log messages show **FCPIO_OUT_OF_RESOURCE**
	The following stats also display incremental readings:
	• Qerror_proc_cnt stats
	• out_of_exch_cnt stats
		No known workaround
		Restarting the host clears the condition.
			3.1(3a)

Open Caveats for Release 3.1(2g)

The following caveats are open in Release 3.1(2g):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCve59744	A vulnerability on TPM 2.0 may occur on Cisco Unified Computing M4 and M5 servers.	It is possible to work-around this TPM issue by generating an RSA key pair externally to the TPM using a trusted generation scheme, and then importing the private key into the TPM using standard TPM 2.0 interfaces and commands. Please also remember to Clear the TPM of existing RSA keys upon either firmware update or utilization of the above work-around as that will ensure that weak keys are no longer employed.	3.1(2g)B
CSCvd90095	UCS VIC 1225 adapter may get stuck in a Pending Next Boot state during a software upgrade.	There is no known workaround.	3.1(2g)C

Open Caveats for Release 3.1(2f)

The following caveats are open in Release 3.1(2f):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCve68431	UEFI Boot Parameters may not be applied on B200 M3 and M4 servers with 3.1(2f).	Manually add the UEFI boot path as a new entry in the BIOS or choose the path through the EFI shell with the steps below. **1.** During the server boot, choose F6 to select Boot Order. **2.** Choose UEFI: Built-in EFI Shell **3.** This will drop you into a CLI shell. **4.** Enter fs0: (Note: this is a zero) **5.** Enter cd efi\boot **6.** Enter ls to list the efi boot files. You should see a file titled BOOTX64.EFI **7.** Enter BOOTX64.EFI - This should load the OS and correct the UEFI boot options.	3.1(2f)B Resolved in 3.1(3f)B
CSCvd05543	For Cisco B460 M4 and B260 M4 Blade servers, without a change to the PWRSEQ_FAULT_N logic from PWRSEQ_WARN_N to Pwr fault may result in a discovery failure if the master and slave blades have different board controller versions.	There is no known workaround.	3.1(2f)B Resolved in 3.1(2g)B
CSCvd42163	During a Fabric Interconnect upgrade or reload, the following error may occur. `ERROR: bootflash: has unrecoverable error; please do "format bootflash:"`	There is no known workaround.	3.1(2f)A Resolved in 3.1(2g)A

Open Caveats for Release 3.1(2c)

The following caveats are open in Release 3.1(2c):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvc68805	SAS Expander Firmware did not upgrade from an earlier release to 3.1(2b), 3.1(2c) and 3.1(2e). **Note** This issue is only applicable for hybrid and All Flash HX240 nodes.	Cisco strongly recommends that you upgrade server firmware C-bundle to 3.1(2f). Or, try the following: • If you upgrade to releases 3.1(2b), 3.1(2c) or 3.1(2e) exclude SAS Expander from your host firmware pack. • You will not encounter any issues if you upgrade to releases 3.1(2f) or 3.1(2g).	3.1(2c)A
CSCvc95647	UCS Manager may incorrectly report the following low memory warning on blade servers with KVM mounted scriptable vMedia: `F1704 275625 sys/chassis-x/blade-y/mgmt/health Health Warning <date> CimcLowMem : Please check the Health tab for more details`	There is no workaround for this alert to be avoided with the current version. Stop using scriptable vMedia, and Linux will eventually reclaim the Cisco IMC memory.	3.1(2c)B Resolved in 3.1(2f)B
CSCvc29340	The Cisco UCS 2304 I/O Module may reboot and generate a kernel core due to a CPU soft lockup.	There is no known workaround.	3.1(2c)A Resolved in 3.1(2f)A
CSCvh97755	Cisco UCS 6200 Series Fabric Interconnect does not pass EAPOL-Start frames from the vEthernet interface to the upstream uplink port in the switch.	There is no known workaround.	3.1(2c)A Resolved in 3.2(3h)
CSCvm89871	Under certain configuration sequences, Cisco UCS Manager managed Blade Servers failed discovery on Fabric Interconnect 6332/6332-16UP. The Tx transmit counter connected to the rack server FI port fails to increment.	1) Connect the cables between FI and rack server (in powered on state) 2) Configure the FI port type as Uplink 3) Then configure the port type as Server	3.1(2c)A Resolved in 3.2(3k)

Open Caveats for Release 3.1(2b)

The following caveats are open in Release 3.1(2b):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvb88279	Boot speeds may be slow when using a storage profile for Pool LUNs on EMC VNX arrays.	Reconfigure/change LUN ownership boot policy so owning SP's are always used above non-owning. Use RAID Group based LUN rather than Pool based LUN. Use a local boot option such as Flexflash or local HDD/SSD.	3.1(2b)B Resolved in 3.1(3f)B
CSCve34690	A FlexFlash Failure may report a "missing" fault for functional SD cards.	Reboot the host to boot from the seond SD Card to see if mirrored configuration was previously present. Configure a call home level of "informational" to receive equipment missing faults.	3.1(2b)A Resolved in 3.1(3d)A
CSCvd56914	Microcode was added for Broadwell and Haswell EX processors support.	There is no known workaround.	3.1(2b)B Resolved in 3.1(2h)B
CSCvd80748	For Cisco B260 or B460 Blade servers, the enable COD setting may cause an incorrect microcode version to appear.	There is no known workaround.	3.1(2b)B Resolved in 3.1(2h)B
CSCvd68198	Microcode was added for E5 Xeon v4 Processor support.	There is no known workaround.	3.1(2b)B Resolved in 3.1(2h)B
CSCuz76350	Cisco B260 or B460 M4 servers running RHEL 6.7 may hang when booting with all the DIMM slots fully populated.	Workaround: Redhat has published this article https://access.redhat.com/solutions/2999221 on how to disable the edac_core and sbridge_edac modules which addresses the hang issue.	3.1(2b)B Resolved in 3.1(3a)A
CSCvb63893	In a Cisco UCS Manager managed environment, the disk inventory may not refresh all the disks present on the system after a power cycle.	Try a manual retry or refresh of the disk inventory.	3.1(2b)C Resolved in 3.1(2f)C

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvb52847	On a B200 M4 blade platform, instead of a NVMe plane, if RAID card is plugged in, then the /var/log/messages file may show "Mux write error" messages. Apart from /var/log/message flood, no functional impact to normal storage operations are noticed.	There is no known workaround.	3.1(2b)B Resolved in 3.1(2f)B
CSCvb69390	Value of "Input Discards" may also count the value of "snmpIfOutDiscards" of the HW counter along with "snmpIfInDiscards".	Do not rely on the "Input Discards" value of "show interface counter". Instead look for the hardware internal counters to know the exact parameter that is incremented. `show hardware internal bcm-usd port-stats slot-num 0 front-port <>`	3.1(2b)A Resolved in 3.1(2f)A
CSCvc03033, CSCvc31880, CSCvc06578, CSCvc85609	When all the UCS Blades are powered on at once, a server may fail discovery with an insufficient power error.	Change the server cap to priority 5.	3.1(2b)A Resolved in 3.1(2f)A
CSCvd24330	IOM backplane down call home alerts (F1797) may be triggered when a blade is rebooted or shut down.	The severity of the backplane port down alert is major so the alert level on the call home profile can be changed to critical to stop receiving these alerts.	3.1(2b)A Resolved in 3.1(2f)A
CSCvb21029	The PSx_STATUS may enter into a failed state for 30 seconds when the PSx is powered off by pwrmgr.	To prevent this from occurring, do the following: • Use a grid policy, so that no PSU needs to be shutdown. • Remove PSUs that are not needed.	3.1(2b)A Resolved in 3.1(2e)A
CSCvb16804	Booting from SAN to a 4K UEFI target may fail.	There is no known workaround.	3.1(2b)B Resolved in 3.1(2e)B
CSCvb95978	On C460 M4 servers, TPM version 1.2 may fail to initialize after installing ESXi OS, and enabling and activating TPM and TXT.	There is no known workaround.	2.2(8d)B Resolved in 3.1(2e)B

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvb44879	An IOM may experience a reboot loop during an upgrade on a setup with a single IOM in the chassis.	If the upgrade has not been started upgrade yet, insert the IOM onto the other side and wait for 15 minutes. Then start the upgrade. If the upgrade has already finished, move the IOM to the other side.	3.1(2b)B Resolved in 3.1(2e)B
CSCvb81317	Fabric interconnect may continuously dump the stack trace on the console after an upgrade to UCS Manager 3.1(2).	If this issue occurs, reboot the FI.	3.1(2b)A Resolved in 3.1(2e)A
CSCvb20365	In Cisco UCS C3x60 server nodes, during the booting of the host, and when the host fails to boot to an OS, Cisco UCS Manager marks the controller as unresponsive because Cisco IMC fails to keep the controller functional.	If this issue occurs, reboot the host and let it boot to the OS.	3.1(2b)A
CSCva61443	In a Cisco UCS C3260 system, when multiple zoning operations are running simultaneously, Cisco UCS Manager disk inventory shows incorrect slot/disks from the server storage inventory randomly.	If this issue occurs, reboot the CMC or AC cycle the chassis.	3.1(2b)C
CSCva28947	In a Cisco UCS C3260 system, when a drive is set to power-save mode, drive firmware update fails with an `IMAGE_BAD_MISMATCH` error.	If this issue occurs, do the following: 1. Change power-policy to "Active" mode. 2. Reboot the host (if the drive is assigned and in power-save mode)	3.1(2b)A
CSCuz41121	When booting to RHEL or running system stress tests, Cisco UCS B420 M4 servers with certain Intel® E5 v3 CPUs may report QPI Correctable System Event Logs with the following error message: `Link Layer CRC successful reset with no degradation` These System Event Logs are benign and do not impact system operation.	There is no known workaround.	2.2(8a)B

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvb16453	The chassis adapter for a Cisco UCS 3260 chassis accepts adapter firmware earlier than Release 3.1(2) when directly updating firmware on the chassis adapter endpoint.	It is highly recommended to upgrade Cisco UCS 3260 chassis endpoints, including shared adapter, using a chassis firmware pack, where we restrict downgrade to bundles earlier than Release 3.1(2). If using direct update of these endpoints, verify and use the appropriate chassis adapter firmware from Release 3.1(2) and later releases.	3.1(2b)A
CSCuz76717	The ESX host reboot hangs while loading the ENIC module with NetFlow enabled.	If this issue occurs, do the following: **1.** Disable NetFlow **2.** Reboot the system **3.** Enable NetFlow	2.2(8a)B 2.2(8a)C
CSCuz79138	The host becomes unresponsive when using second generation VIC adapters while running FCOE traffic and Ethernet traffic on the same side of the fabric with NetFlow enabled.	No known workaround for second generation VIC adapters. You can enable NetFlow with third generation VIC adapters or later generation adapters.	2.2(8a)B 2.2(8a)C
CSCvb34628	In rare cases, firmware update of the storage controller fails with a flash programming error. This will result in the rare occurrence of a failed controller requiring RMA. **Note** This issue occurs while battery/super capacitor relearn cycle is in progress, and the relearn completes before the flash write is complete.	If this issue occurs, do the following: **1.** Check the status of the battery/super capacitor learn cycle and wait for it to finish. **2.** Ensure that the "Next learn time" is not anytime in the next hour before issuing the firmware update.	3.1(2b)C

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvb35827	Upgrade failure occurs when the Cisco UCS system is configured with more than 128 LDAP groups and upgrade is performed either from Cisco UCS Manager Release 2.2.8 to Cisco UCS Manager Release 3.1(2b) or from Cisco UCS Manager Release 3.1(2b) to a later release. The following error message is displayed: `Error: Update failed: [System has more than 128 LDAP groups set, Downgrade will cause ldapd crash, Delete the additional groups]`	If this issue occurs, do the following: 1. Create a backup of the configuration and reduce the number of LDAP groups to a value below or equal to 128. 2. After upgrade, re-apply the configuration.	3.1(2b)A
CSCux11611	Seagate hard drives left spinning idle without an operating system installed or setup with the JBOD configuration without read or write activity are prone to failure. Impacted hard drives are listed here: • UCS-HD4T7KS3-E • UCSC-C3X60-HD4TB (4TB) • UCS-HDD3TI2F214 (3TB) • UCS-HDD2TI2F213 (2TB) • UCS-HDD1TI2F212 (1TB) • UCS-HD6T7KL4K • UCSC-C3X60-HD6TB • UCSC-C3X60-6TBRR	Do not leave idle systems powered on for extended periods of time. Either install an OS with all drives formatted or configure drives in a RAID configuration other than JBOD or JBOD equivalent and fully initialize the Virtual Drive(s).	2.2(7c)B Resolved in 3.1(2c)B
CSCvf33668	While upgrading the infrastructure firmware using AutoInstall from 3.1(2b) to 3.1(2f) in a system where UCS 2304 IOMs are connected to Cisco UCS 6300 Series FIs using copper 40G QSFP cables, the IOMs are marked as offline and then come back online on their own in a couple of minutes.	No known workaround for this issue.	3.1(2b)

Open Caveats for Release 3.1(1k)

The following caveats are open in Release 3.1(1k):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCva17840	System configured with single path iSCSI fails to boot to RHEL 6.8 with kernel panic or an iSCSI connection error message.	Use multipath iSCSI boot configuration for RHEL 6.8 to boot successfully.	3.1(1k)A
CSCux96072	During heavy I/O traffic, the Cisco 12G Modular RAID controller may go offline with the Storage Controller SLOT HBA inoperable error logged in the Cisco IMC event logs.	A fix is available in UCS Manager 2.0.10e and 2.0.13. Upgrade the Storage controller firmware and its corresponding driver.	2.2(6e)C Resolved in 3.1(1k)C

Defect ID	Symptom	Workaround	First Bundle Affected
CSCva47085	When using VIC1340 with 2304 IOM Native 40G backplane connection (not 4x10G), LUNs disconnect or failure occurs during FC/FCOE reboot. In the VMware vmkernel log the following message may be seen: `2016-06-21T04:32:36.106Z cpu25:33191)<3>fnic : 2 :: hdr status = FCPIO_DATA_CNT_MISMATCH` In the VIC adapter log the following message may be seen: `160621-04:26:51.733255 ecom.ecom_main ecom(8:3): ox_id 41d4 rx_id 44b seq_cnt 7 seq_id 1 160621-04:26:52.066235 ecom.ecom_main ecom(8:1): fcpio_data_cnt_mismatch for exch 4202 status 1 rx_id5f7 s_stat 0x3 xmit_recvd 0x3000 burst_offset 0x3000 sgl_err 0x0 last_param 0x2800 last_seq_cnt 0x0 tot_bytes_exp 0x8000 h_seq_cnt 0x5 exch_type 0x0 s_id 0xab800 d_id 0xab800 host_tag 0x377` Non-stomped CRC is observed coming from the IOM to adapter. The following messages may be seen in the Cisco UCS Manager CLI: `connect adapter x/x/x attach-mcpdcem-macstats 0 <- check for "Rx CRC error frames not stomped" dcem-macstats 1 <- check for "Rx CRC error frames not stomped"`	If this issue occurs do one of the following: • With VIC1340 use 4x10G only, by removing the port expander. • Use the VIC1380 adapter only.	3.1(1e)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCux66914	When changing the Chassis Connect Policy to 'Port-Channel', some fabric ports may go to failed state with the following message: `SDP timeout/SFP Mismatch` This may also potentially happen during IOM bootup time or under situations which lead to a flap of the fabric ports. **Note** This is applicable only to passive copper cables.	If this issue occurs do one of the following: • Change Chassis Connect Policy to 'non-Port-Channel' and then back to 'Port-Channel'. • Reset IOM.	3.1(1e)A

Open Caveats for Release 3.1(1h)

The following caveats are open in Release 3.1(1h):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvg16805	In a setup with a 6332-16UP FI, a 5108 blade chassis, and IOM 2304, with one 40G link from IOM to FI, the subordinate IOM goes offline for 30-40 seconds when a chassis techsupport is requested.	There is no known workaround for this issue.	3.1(1h)A Resolved in 3.2(3a)A
CSCvf40571	Service profile association fails after FI failover from FI A to FI B and the Associate FSM remains at the ComputePhysicalAssociateSwConfigHostOSPeer stage under the following conditions: • It is a High Availability setup with the server discovered from both ends (connection status: A, B) • Server is associated and powered off. • The FI, which is the managing instance of the adaptor(s) on this server, is brought offline. After some time, this server goes into re-association and remains at the ComputePhysicalAssociate:SwConfigHostOSPeer stage with status as 'FAILED'. This continues until the FI is brought back up.	When this issue occurs, do the following: • Bring up the FI that has gone down • Reacknowledge the affected server	3.1(1h)A Resolved in 3.2(3a)A
CSCve41380	The operating system may fail to boot when one of the SD cards in a RAID 1 configuration is inoperable.	Remove the failed SD card and then replace it with a working SD card.	3.1(1h)B Resolved in 3.1(3d)B

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvb68147	The IOM may go offline when the host interface links are down and under constant temperature change.	There is no known workaround.	3.1(1h)A Resolved in 3.1(2g)A
CSCuz69678	While upgrading Cisco UCS Manager from release 2.2(8) to 3.1(1) with 128 LDAP groups configured, the system generates the following critical fault: `[FSM:FAILED]: user configuration (FSM:sam:dme:AaaUserEpUpdateUserEp). Remote-Invocation-Error: SAM coupler version not supported.`	When this issue occurs, acknowledge the reboot for the Fabric Interconnect. As a result, UCS will have the same version for Cisco UCS Manager and NXOS. The fault will be cleared.	3.1(1g)A

Open Caveats for Release 3.1(1g)

The following caveats are open in Release 3.1(1g):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvb93881	IOM 2300 and UCSB-5108-AC2 chassis may display the fault F0409 "Thermal condition on chassis x is upper-critical". **Note** This has no operational impact but could generate call home alerts.	There is no known workaround.	3.1(1g)A Resolved in 3.1(2h)A
CSCva67630	False SER errors may occur for FP ternary content addressable memory (TCAM) tables for Cisco UCS 6300 Series Fabric Interconnects.	Consider the reboot request if the error is fatal or if errors occur in one of the tables below. • fp_gm_fields • fp_global_mask_tcam All remaining reboot notifications should be ignored. The tables in which an error has occurred can be found out from the command below. `show logging onboard bcm_usd | grep error`	3.1(1g)A Resolved in 3.1(2g)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvb90616	Fabric Interconnect may crash during an image upgrade due to memory corruption with the following error: `SMI: System watchdog timed out`	If you encounter this issue, power cycle the system.	3.1(1g)A Resolved in 3.1(2e)A, 3.1(1l)A
CSCva36811	When logging into Cisco UCS Manager through HTML5, if a password length greater than 32 characters is configured, the following authentication error may appear: `Login Error: Authentication failed`	If you encounter this issue, use a maximum password length of 32 characters.	3.1(1g)A Resolved in 3.1(1l)A
CSCvb90517	Both fabric interconnects may reboot with vim hap reset reason codes.	There is no known workaround.	3.1(1g)A Resolved in 3.1(2e)A, 3.1(1l)A
CSCux35404	While performing a backup on Cisco UCS B200 M4 servers, the vNICs are disconnected from the OS. Core files may also be generated.	When this issue occurs, reboot the blade server to re-establish connectivity through the adapter.	3.0(2d)
CSCuz97205	Server reboots once when any trivial change is made on the service profile. Purpose property change on adaptorHostFcIf causes the server to reboot.	If the maintenance policy is set to user-ack for the service profile, the server will go into maintenance permission and would not directly go for a reboot.	3.1(1g)A Resolved in 3.1(1k)A
CSCux53224	A fatal error may be observed when you create or remove virtual drives with RAID 5 and RAID 6 controller combination.	No known workaround.	3.1(1g)C Resolved in 3.1(1k)C

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuz40326	When there is a database load, in operations such as DME restart, failover, reboot, firmware upgrade, the assigned IP's in a pool used by iSCSi vNICs will get unassigned. This may result in the same IP from the pool to be assigned to different endpoints. In addition transaction failures may occur, since an endpoint will try to use an IP that is already assigned. The following failures may occur in this scenario: • Upgrade fail with validation error. • Unresponsive/inapplicable status of an FI due to DME transaction failing consistently. • GUI still shows the old verison while CLI shows the new version number. • After primary FI is rebooted, it may show mgmt service is not ready. Cluster comes up as `"Management services: INIT IN PROGRESS" and mgmt services state:INVALID although subordinate FI shows that mgmt services is up.`	When this issue occurs perform the following procedure in Cisco UCS Manager: 1. In the Navigation pane, click the Servers tab. 2. On the Servers tab, expand Servers > Service Profiles. 3. Expand the node for the organization that contains the service profile from which you want to delete an iSCSI vNIC. 4. Expand the service profile from which you want to delete an iSCSI vNIC. 5. Expand the iSCSI vNICs node. 6. Right-click the iSCSI vNIC you want to delete and choose Delete. 7. If the Cisco UCS Manager GUI displays a confirmation dialog box, click Yes.	3.1(1g)A Resolved in 3.1(2b)A

Open Caveats for Release 3.1(1e)

The following caveats are open in Release 3.1(1e):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvm02934	Cisco UCS B-Series M2 servers are based on Intel® processors that are vulnerable to exploits that use CPU speculative processing and data cache timing to potentially identify privileged information. These exploits are collectively known as L1 Terminal Fault (L1TF). • CVE-2018-3615 (affecting SGX), also known as Foreshadow, is not known to affect any existing Cisco UCS servers because Cisco UCS M5 and earlier generation servers, and HyperFlex M5 and earlier generation servers do not use Intel® SGX technology. • CVE-2018-3620 (affecting OS/System Management Mode) and CVE-2018-3646 (affecting Virtual Machine Monitors) are referred to as L1 Terminal Fault attacks by Intel®. These vulnerabilities are mitigated by applying the updated processor microcode from Intel included in the server firmware bundle, and the relevant Operating System and Hypervisor patches from the appropriate vendors.	The fix for CVE-2018-3620 (OS/SMM) and CVE-2018-3646 (VMM) requires applying the updated processor microcode from Intel® as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. For more information, please see the Cisco Security Advisory available here: CPU Side-Channel Information Disclosure Vulnerabilities: August 2018	3.2(1d)B, 3.2(1d)C 3.1(1e)B, 3.1(1e)C 2.2(1b)B, 2.2(1b)C CSCvm02934 is resolved in 3.1(3j)B, 3.1(3j)C

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvm03356	Cisco UCS B-Series M3 servers and C-Series M3 servers are based on Intel® processors that are vulnerable to exploits that use CPU speculative processing and data cache timing to potentially identify privileged information. These exploits are collectively known as L1 Terminal Fault (L1TF). • CVE-2018-3615 (affecting SGX), also known as Foreshadow, is not known to affect any existing Cisco UCS servers because Cisco UCS M5 and earlier generation servers, and HyperFlex M5 and earlier generation servers do not use Intel® SGX technology. • CVE-2018-3620 (affecting OS/System Management Mode) and CVE-2018-3646 (affecting Virtual Machine Monitors) are referred to as L1 Terminal Fault attacks by Intel®. These vulnerabilities are mitigated by applying the updated processor microcode from Intel included in the server firmware bundle, and the relevant Operating System and Hypervisor patches from the appropriate vendors.	The fix for CVE-2018-3620 (OS/SMM) and CVE-2018-3646 (VMM) requires applying the updated processor microcode from Intel® as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. For more information, please see the Cisco Security Advisory available here: CPU Side-Channel Information Disclosure Vulnerabilities: August 2018	4.0(1a)B, 4.0(1a)C 3.2(1d)B, 3.2(1d)C 3.1(1e)B, 3.1(1e)C 2.2(1b)B, 2.2(1b)C CSCvm03356 is resolved in 3.1(3j)B, 3.1(3j)C

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvm03351	Cisco UCS B-Series M4 servers, C-Series M4 servers, S3260 M4 storage servers, and HyperFlex M4 servers are vulnerable to exploits that use CPU speculative processing and data cache timing to potentially identify privileged information. These exploits are collectively known as L1 Terminal Fault (L1TF). • CVE-2018-3615 (affecting SGX), also known as Foreshadow, is not known to affect any existing Cisco UCS servers because Cisco UCS M5 and earlier generation servers, and HyperFlex M5 and earlier generation servers do not use Intel® SGX technology. • CVE-2018-3620 (affecting OS/System Management Mode) and CVE-2018-3646 (affecting Virtual Machine Monitors) are referred to as L1 Terminal Fault attacks by Intel®. These vulnerabilities are mitigated by applying the updated processor microcode from Intel included in the server firmware bundle, and the relevant Operating System and Hypervisor patches from the appropriate vendors.	The fix for CVE-2018-3620 (OS/SMM) and CVE-2018-3646 (VMM) requires applying the updated processor microcode from Intel® as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. For more information, please see the Cisco Security Advisory available here: CPU Side-Channel Information Disclosure Vulnerabilities: August 2018	4.0(1a)B, 4.0(1a)C 3.2(1d)B, 3.2(1d)C 3.1(1e)B, 3.1(1e)C 2.2(1b)B, 2.2(1b)C CSCvm03351 is resolved in 3.1(3j)B, 2.2(3j)C

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvj59299 CSCvj59301	Cisco UCS B-Series and C-Series M2 servers are based on Intel® Xeon® 5500, 5600, and EX series processors that are vulnerable to variants of an exploit that uses CPU speculative processing and data cache timing to efficiently leak information, known as Spectre. CVE-2018-3639 (Spectre/Variant #4) and CVE-2018-3640 (Spectre/Variant #3a) are addressed by relevant Operating System patches using an interface provided by updated processor microcode included in the server firmware bundle.	The fix for CVE-2018-3639 (Spectre/Variant #4) and CVE-2018-3640 (Spectre/Variant #3a) requires applying the updated microcode from Intel as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. For more information, see the Cisco Software Advisory at: CPU Side-Channel Information Disclosure Vulnerabilities: May 2018	3.1(1e)B, 3.1(1e)C 3.2(1d)B, 3.2(1d)C 2.2(1b)B, 2.2(1b)C CSCvj59299 is resolved in 3.1(3j)B and 3.1(3j)C

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvj54880 CSCvj54847 CSCvj54187	Cisco UCS M3 and M4 servers, and Hyperflex M4 servers are based on Intel® processors that are vulnerable to variants of an exploit that uses CPU speculative processing and data cache timing to efficiently leak information, known as Spectre. CVE-2018-3639 (Spectre/Variant #4) and CVE-2018-3640 (Spectre/Variant #3a) are addressed by relevant Operating System patches using an interface provided by updated processor microcode included in the server firmware bundle.	The fix for CVE-2018-3639 (Spectre/Variant #4) and CVE-2018-3640 (Spectre/Variant #3a) requires applying the updated microcode from Intel as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. For more information, see the Cisco Software Advisory at: CPU Side-Channel Information Disclosure Vulnerabilities: May 2018	3.1(1e)B, 3.1(1e)C 3.2(1d)B, 3.2(1d)C 2.2(1b)B, 2.2(1b)C 3.0(1c)B, 3.0(1c)C - Only for M3, M4 EP Resolved in 3.1(3j)B and 3.1(3j)C
CSCvh22485	After a vMotion or virtual machine migration in a VMFEX setup, virtual machines may be unable to receive broadcast or multicast packets, including ARP packets. The issue has been resolved.	Do not perform a vMotion or VM migration. If needed, power-off, migrate the VM, and then power-on again. If the issue happens again, power cycle the VM after vMotion.	2.2(8g)A Resolved in 3.1(3f)A
CSCvg44307	Stale entries in IOM may cause a communication failure within the same VLAN and fabric interconnect.	Reboot the IOM to recover from this condition.	2.2(4b)A Resolved in 3.1(3f)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuw09993	ESXi may report a fatal error while loading /s.v00 during the "Loading VMware Hypervisor" Screen.	Ensure that your primary boot path is the SAN boot LUNs "Optimized Path" to the array. If the issue is encountered, this means that the LUN was sitting on a "Non-Optimized Path" and failed when the implicit transfer occurred to make it the "Optimized Path". Since the boot path is now the "Optimized Path" a reboot will result in the OS booting properly this time.	2.2(3a)B Resolved in 3.1(3f)B
CSCvg44307	Communication may fail within the same VLAN and FI for two hosts that are part of the same chassis. The same devices were able to communicate with other devices within the same VLAN but not with each other.	Reboot the IOM to recover from this condition.	2.2(4b)A Resolved in 3.1(3f)A
CSCvg98077	During a TPM firmware update, the process may be interrupted by a UCS Manager event. If this event occurs, the TPM firmware flash may fail, resulting in a unresponsive state.	There is no known workaround.	2.2(8i)B Resolved in 3.1(3f)B
CSCvf59328	The fNIC no longer reports DATA_CNT_MISMATCH when the TASK_SET_FULL SCSI command is received from the storage array.	There is no known workaround.	3.1(1e)B Resolved in 3.1(3f)B
CSCvd54828	The RAID controller may encounter an error and resets. This may occur when an external SATA solid state drive (SSD) is used instead of a SAS SSD.	There is no known workaround.	3.0(3a)C Resolved in 3.1(3d)C

Defect ID	Symptom	Workaround	First Bundle Affected
CSCve23500	UCS B200 M4 Bladeserver may crash with SD Card Connectivity issues.	The FlexFlash Scrub needs to be performed with the following steps. Warning: Scrubbing will erase the contents of SD card. 1. Enable FlexFlash Scrub in the Scrub Policy / Create a new Scrub Policy with FlexFlash Scrub set to 'Yes' and use it in Service Profile 2. Server Maintenance -> Re-acknowledge 3. Once Server discovery and re-association finishes, set FlexFlash Scrub to 'No' in Scrub Policy used in the Service Profile.	2.2(3d)B Resolved in 3.1(3d)B

Defect ID	Symptom	Workaround	First Bundle Affected
CSCve14926	The following configuration error occurs while associating a service profile with UCSC-C240M4-SX or UCSC-C240-M4L servers: `Controller does not support out of band configuration Controller sys/<rack-unit-[the rack server id]>/board/storage-PCH-1 does not support OOB` This error occurs only when the following conditions are met: • The server has internal SSD(s) in slot 1 and 2 of the internal riser card, which are managed by the onboard PCH controller • The server has disks in external slot 1 and slot 2, which are managed by PCI slot based storage controller • The disk group policy, configured in the service profile, is set as Disk Group Configuration (Manual) • External disks 1 and 2 are selected in the manual disk group policy	Configure the disk group policy as **Disk Group Configuration (Automatic)**.	3.1(1e)A Resolved in 3.1(3c)A
CSCvd91302	UCS Mini and the Fabric Interconnect may loose connection after a change in the MTU value in BM and DQ.	Reload the fabric interconnect.	3.1(1e)A Resolved in 3.1(3b)A, 3.1(2h)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCva31113	After a fabric interconnect reboot, a file system corruption may occur on systems that contain an Indilinx controller.		2.1(1a)A Resolved in 3.1(2h)A, 3.1(3b)A

Defect ID	Symptom	Workaround	First Bundle Affected
		In most cases the underlying file system corruption can be fixed by booting into the kickstart image and running a file system check. A pre-upgrade package containing a script and a kernel module was developed for 62xx Fabric Interconnects running 2.2(x) firmware to ensure proper SSD shutdown prior to the reboot required during the upgrade process. With this deployed, the risk to run into a file system corruption issue during reboot is reduced, however not eliminated. There is no guaranteed preventative workaround. Although corruption may still occur, it is recommended to use the pre-upgrade package to send proper SSD shutdown commands prior to reboot. Please contact Cisco TAC for assistance with recovery or the pre-upgrade script. **Note** The pre-upgrade	

Defect ID	Symptom	Workaround	First Bundle Affected
		script will NOT work on 61xx FIs or 2.1(x) UCS firmware.	
CSCuv43292	The fabric interconnect may crash due to a sleeping function called within an interrupt context.	There is no known workaround.	Both 2.2(4a) and 2.2(5a) are affected but not 2.2(6), 2.2(7), and 2.2(8). Resolved in 3.1(2h)A
CSCvd54116	Setting a custom cipher suite for UCSM may result in a "handshake failure" error message when attempting to open a Java login to UCSM or a KVM session to a blade server.	Explicitly allow AES128-SHA in the custom cipher to allow login to UCS Manager. This only affects the UCS Manager Java GUI. However if a KVM session is opened, then the failure will be seen as well, as this is still uses Java.	2.2(8c)A Resolved in 3.1(2h)A
CSCvb14641	Power policies may be out of synchronization between UCS Manager and CMC after the master IOM is rebooted.	Force a PSU redundancy config deployment from UCS Manager then flip the policy to GRID and back.	3.0(2c)A Resolved in 3.1(2h)A, 3.1(3a)A
CSCvb61558	UCSB-PSU-2500ACDV may display incorrect power readings in the PSMI register.	There is no known workaround.	3.1(1e)A Resolved in 3.1(2h)A
CSCvb92941	UCS-IOM-2304 may fail to capture kernel cores in the obfl_raw partition.	There is no known workaround.	3.1(1e)A Resolved in 3.1(2h)A
CSCvd93200	A random reboot due to a spinlock lockup may occur on Cisco UCS 2304.	There is no known workaround.	3.1(1e)A Resolved in 3.1(2h)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCva89402	An incorrect fault may be generated in UCS Manager when the power supply input source shows "unknown".	There is no known workaround.	3.1(1e)B Resolved in 3.1(2h)B
CSCvc99135	The UCS Fabric Interconnect generates IGMP proxy reports where the source mac address of the data packets is replaced by the Fabric Interconnect, but the IP address is still the same as the VM. The data packets reach the upstream switch with the same IP address. This creates multiple entries in the IP-mac table for the IP in the uplink switch, which results in end point movement.	There is no known workaround.	3.1(1e)B Resolved in 3.1(3a)B
CSCvd71484	The 6332 Fabric Interconnect input error counter may display a very high value for the port-channel interface.	When this issue occurs, do one of the following: • Clear the counters by using the NxOS CLI command **clear counters** • Ignore the Input Error Count on the port-channel and use the Input Error Count(s) of the members of the port-channel.	3.1(1e)A

CSCvd24782	When the poweroff module is available for less than 15 seconds, all of the poweron commands time out. The poweroff module <module_number> is then seen in the list of installed features on the FI through NXOS:
	`version 5.2(3)N2(2.27b)`
	`feature fcoe`
	`poweroff module 4`
	The module appears to no longer work after it reboots.
		When this issue occurs, do the following:
		1. Contact TAC to load the debug plugin and power the module on manually
		2. Reboot the FI
			3.1(1e)A
			Resolved in 3.1(3a)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvb93384	When running the vnic placement tests through multiple iterations, the HIF port may intermittently encounter an error.	The port auto recovery mechanism should be enabled. If any HIF port encountered the error-disabled state, the port should automatically recover in 60 seconds.	3.1(1e)B
CSCvd42163	During a Fabric Interconnect upgrade or reload, the following error may occur. `ERROR: bootflash: has unrecoverable error; please do "format bootflash:"`	There is no known workaround.	3.1(1e)A Resolved in 3.1(2g)A
CSCvd20170	A Cisco UCS Manager power group change implemented through the HTML5 GUI may show 0W for a blade server in the chassis.	Perform the power group change through the Java GUI or CLI.	3.1(1e)A Resolved in 3.1(2g)A
CSCvc02297	The power cap application may fail for a Bladeserver when the server is powered on or off from outside of Cisco UCS Manager.	The fault can be ignored. During the maintenance window, shutdown the Bladeserver from the OS and power on the server from the UCS Manager GUI or CLI.	3.1(1e)A Resolved in 3.1(2g)A
CSCvb79455	The critical fault code F1000227 may occur on both the primary and subordinate FI during upgrade.	This issue can occur when the expansion module from the FI was removed. Reinsert the GEM card back to the previous slot.	3.1(1e)A Resolved in 3.1(2g)A
CSCvc05615	FI-6396UP with FC 16G interfaces (individual/port-channel) may incorrectly report discard frame count. The issue was a cosmetic one where-in the discard count (both input and output) used to increase every few minutes. The interfaces themselves are not impacted and remain up.	There is no known workaround.	3.1(1e)A Resolved in 3.1(2g)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvc46313	The remote operation of making the LUN online from UCS Central may fail with the error message: `Global Service profile [org-root/org-GKDC/org-<name>/ls-SP_3260_03] can not be modified from UCS domain. Please make the changes from UCS Central that you are registered with.`	Contact Cisco TAC for a workaround.	2.2(4b)A Resolved in 3.1(2f)A
CSCva14937	M4 blades installed with SD cards instead of a hard disk may halt at 'Local Drive' for automated deployments with the following boot policy: Boot Policy • CD/DVD • Local Drive • Network Adapter (PXE)	There is no known workaround.	2.2(3f)B Resolved in 3.1(2f)B
CSCva35757	Latency between the UCS Manager Client and fabric interconnect may cause the firmware page to load slowly.	Use the CLI to complete upgrade and downgrade procedures.	2.2(7b)A Resolved in 3.1(2f)A
CSCvb22090	During a disk firmware upgrade, when an unconfigured bad drive is encountered, the upgrade may stop and the remaining drives on the UCS Rack server are not updated.	There is no known workaround. Verify that all the hard drives are setup correctly before the firmware update.	2.2(3a)A

CSCvb85331	The following fault may occur after a UCS Manager software upgrade.
	Code: F1781
	Description: Management database version mismatch detected failover may not complete
	Affected Object: sys/mgmt-entity-B
	Name: Mgmt Entity Mgmt Db Version Mismatch
	Cause: Replication Failure
	Type: Management
		Restart the process monitor on the subordinate FI with the following commands:
		`connect local-mgmt (A/B)`
		`pmon stop`
		`pmon start`
		`show pmon state`
			2.2(8c)A
			Resolved in 3.1(2f)A

Defect ID	Symptom	Workaround	First Bundle Affected

CSCvc10791	A DME process may crash when the dynamic vNIC and static vNIC contain a different adminVcon property value.	Collect UCS Manager tech support logs from the local-mgmt CLI and contact TAC.
		`connect local-mgmt`
		`show tech-support ucsm detail`
			2.2(3e)A
			Resolved in 3.1(2f)A

CSCvc14810	Systems with 6300 Fabric Interconnects and Windows Server 2012 virtual machines may experience intermittent packet loss due to missing VLAN translate entries.	Contact TAC for a temporary workaround. A permanent fix is only available for UCS Manager version 3.1(2f) or higher.	3.1(1e)A Resolved in 3.1(2f)A
CSCvc31867	When upgrading the SSD to firmware 32F3Q, the firmware may be truncated and written as 2F3Q, which may cause a second request for the reboot of the server.	Exclude the Local Disk Firmware update from the Host Firmware Package (HFP) in the associated Service Profile.	2.2(8a)A Resolved in 3.1(2f)A
CSCvc39322	For B260 M4 Blades, BIOS v3.1.2.2 may intermittently fail Windows HLK and HCK Trusted Platform Module (TPM) tests on Windows Server 2016 and Windows Server 2012 R2.	Toggle the BIOS "TXT Support" setting to disable.	2.2(7b)B Resolved in 3.1(2f)B
CSCvc46313	Remote operation from UCS Central no longer fails with the error message: `Global Service profile [org-root/org-GKDC/org-<name>/ls-SP_3260_03] can not be modified from UCS domain. Please make the changes from UCS Central that you are registered with.`	Workaround: There is no known workaround. Contact TAC for assistance.	2.2(4b)A Resolved in 3.1(2f)A
CSCvc60876	The 6248, 6296, and 6332 Series Fabric Interconnect may send Smart Call Home messages in the wrong format.	Contact the Smart Call Home support team to fix the XML file and reprocess the message.	2.2(8b)A Resolved in 3.1(2f)A

Defect ID	Symptom	Workaround	First Bundle Affected

CSCvc89242	The Fabric Interconnect may reboot due to a CDP process crash.	If CDP still crashes immediately after the fabric interconnect reboot, execute the following commands to avoid another FI reboot.
		`connect nxos`
		`system no hap-reset`
		Contact TAC with the CDP core dump files if the reboot occurs again.
			2.2(6e)A
			Resolved in 3.1(2f)A

CSCva71801	UCS Manager may fail to synchronize with the IPv6 NTP server.	If possible, drop into the debug plugin. Restart the process ntpd by issuing the command: `killall ntpd` Or change the IPv6 NTP server to a IPv4 NTP server.	2.2(8a)A Resolved in 3.1(1l)A
CSCuy52691	After upgrading to Cisco UCS Manager Release 3.1(1e), the blade server may fail to power on with the following fault: Description: Insufficient power available to power-on server x/y Affected Object: sys/chassis-x/blade-y/budget Name: Power Budget Power Budget Unavailable	Change the power control policy in Service Profile to "cap" with a default priority value of "5".	3.1(1e)A Resolved in 3.1(1l)A
CSCuu99255	The "show fabric-interconnect inventory expand" command may display the ethernet port with a role of “Unknown” instead of "Server".	The role can be recovered by disabling and enabling the port.	2.1(1a)A Resolved in 3.1(1l)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuy81688	From Cisco UCS Manager tech-support, running /var/sysmgr/sam_logs/httpd_cimc.log on the affected fabric interconnect may show the "exceeded max time without restart" error. From Cisco UCS Manager tech-support, running /ls_l.out on the affected fabric interconnect may show the existence of a 'cimcrestart' file under /isan/apache/conf/. The modified date is now updated.	Using the debug plugin, delete the file /isan/apache/conf/cimcrestart. Stop and start the UCSM processes using 'pmon stop'/'pmon start'.	2.2(8a)A Resolved in 3.1(1l)A, 3.1(2b)A
CSCvb18143	ACL Fabric Manager core maybe seen during Cisco UCS Manager upgrade or downgrade to 3.1(1l) or higher.	There is no known workaround.	2.2(8c)A Resolved in 3.1(1l)A, 3.1(2b)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuz53730	Under heavy load on httpd, either from API, Cisco UCS Central and/or Cisco UCS Manager sessions, Cisco UCS Manager httpd process may experience high memory usage or crash with a core file showing indications of memory allocation failure.	If the issue is encountered, memory usage can be minimised by: • Reducing the volume of simultaneous requests to HTTPD by API polling and open UCSM sessions. Resolving UCS Manager faults (large numbers can cause increased memory usage). • UCSM will automatically restart process until it reaches failure threshold (typically 4). After that, it is advised to failover to the subordinate FI and either reboot or restart management on the previous primary.	2.2(2c)A Resolved in 3.1(1l)A
CSCul97240	When a UCS rack server is present in a UCS setup, DHCP renewal may trigger Information level syslog messages to be sent to the syslog server configured on Cisco UCS Manager.	There is no known workaround.	2.2(1a)A Resolved in 3.1(1l)A
CSCva56277	During downgrade of Cisco UCS Manager A bundle, the slots 3 and 4 in the fabric interconnect may be reported as powered off.	There is no known workaround.	2.2(3a)A Resolved in 3.1(1l)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCva85907	During discovery of Cisco UCS C240 M4 server with Intel x520, Emulex 11102, and Qlogic 844 converged network adapters, the Intel X520 adapter may revert to old firmware after a successful host firmware package (HFP) update.	There is no known workaround.	3.1(1e)A Resolved in 3.1(1l)A, 3.1(2b)A
CSCva38476	An infrastructure software upgrade to UCS Manager 2.2(7b) or higher may fail when both fabric interconnects are incompatible or when one of the fabric interconnects is unresponsive.	If you encounter this issue, contact TAC to apply a workaround.	2.2(7b)A Resolved in 3.1(1l)A
CSCva34343	Cisco UCS Manager may report false alerts due to P0V75_STBY sensor in Cisco B200 and M4 Blade Servers.	There is no known workaround.	2.2(6e)B Resolved in 3.1(1l)B
CSCuz21644	When Internet Explorer 11 browser is used to download the license file through Cisco UCS Manager **Admin** > **License Management** > **Download tasks** > **Download license file** > **Local File System**, the local file system may fail.	If you encounter this issue, try using the Chrome browser as a workaround.	3.1(1e)A Resolved in 3.1(1l)A
CSCva27558	In scenarios such as traffic loops in external networks, a series of MAC add or delete operations may cause the MAC address to display in the software table, and not in the hardware table for all the ASICs.	Avoid traffic loops in the external network. Once the problem is encountered, the MAC address can be manually cleared from the CLI to fix the issue. Example: `ESC-POD-0025-A(nxos)# clear mac address-table dynamic address 0050.56b2.4db2 vlan 205`	2.2(5c)A Resolved in 3.1(1l)A, 3.1(2b)A
CSCva61701	When the Cisco UCS fabric interconnect uplinks are in the individual (" I ") state, broadcast traffic received on one interface may be sent back upstream on the other interfaces.	Set the "suspend individual" value to True in the LACP network policy. This will make sure that the port is suspended (s state) instead of individual (I state).	3.1(1e)A Resolved in 3.1(1l)A, 3.1(2b)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCva73387	The SNMP process may crash and cause the fabric interconnects to reload when DNS is configured on the fabric interconnects and SNMP trap hosts are configured with domain names.	There is no known workaround.	3.1(1e)A Resolved in 3.1(1l)A, 3.1(2b)A
CSCvb11667	Cisco UCS B200 Blade Servers with UEFI BIOS enabled, may fail to SAN boot from a target LUN with an ID other than 0 and using T10 DIF protection.	If this issue occurs, you can set the BIOS to legacy mode or use LUN ID 0.	2.2(8d)B Resolved in 3.1(2e)B
CSCvc17769	The fabric interconnect may crash when the bound interface of a Veth is in the "Not Initialized State" during a VLAN configuration change.	If the bound interface of Veth is not initialized, then do not perform a VLAN configuration change on the Veth.	2.2(7c)A Resolved in 3.1(2e)A, 3.1(1l)A
CSCvb08928	A fabric interconnect may reboot from a VLAN deletion due to a FWM hap reset.	Avoid deleting a VLAN.	2.2(5a)A Resolved in 3.1(1l)A, 3.1(2e)A
CSCvb77811	Fault codes F0369 and F0391 may randomly appear on Cisco UCS 5108 Blade Servers and UCS 2200 Fabric Extenders.	Remove a PSU from the chassis, so that chassis doesn't have extra PSUs to turn off or on. You can also ignore the fault. This won't affect functionality as long as the chassis power consumption does not exceed 5000w.	3.1(1e)A Resolved in 3.1(2e)A
CSCvb85544	A race condition in the Linux kernel's memory subsystem that handled the copy-on-write (COW) of read-only memory mappings may occur on fabric interconnects.	There is no known workaround.	2.2(1a)A Resolved in 3.1(2e)A, 3.1(1l)A
CSCvc17769	The fabric interconnect no longer crashes when the bound interface of Veth is in the "Not Initialized State" during a VLAN configuration change.	If the bound intf of Veth is in not initialized, do not perform a VLAN configuration change on the Veth.	2.2(7c)A Resolved in 3.1(2e)A, 3.1(1l)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvb82862	EUI-64 bit addresses were invalid when entered for storage connection policies or SAN boot targets.	There is no known workaround.	2.2(8d)A Resolved in 3.1(2e)A, 3.1(1l)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuw50361	While collecting IOM tech-support by using the command "show platform software satctrl global", the HIF/NIF interfaces of an IOM no longer flap due to SDP heartbeat timeout.	If you have encountered this SDP timeout during tech-support collection, take the following actions for any subsequent tech-support on the chassis that had been impacted: • If troubleshooting a blade or host level issue, specify the exact blade in question to only collect the Cisco IMC and adapter logs. Note: The default chassis selection of "CIMC ID: all" will collect IOM logs as well. • If troubleshooting an IOM level issue, TAC can perform a workaround by removing the impacting command "show platform software fwmctrl trace" from the IOM tech-support generation. Contact TAC for additional assistance.	2.2(4b)A Resolved in 3.1(2e)A, 3.1(1l)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvb78971	When attempting the auto-install of UCS Manager, the fabric interconnect upgrade may fail when the /var/tmp usage exceeds 10%.	There is no known workaround.	2.2(3k)A Resolved in 3.1(2e)A, 3.1(1l)A
CSCvb50641	UCS Mini backplane port may go down after firmware check fails.	• Option 1: At the NxOS command prompt enter: test hardware internal mtc-usd load_ucode front-port X where X is the port number. • Option 2: For the affected interface, at the NxOS command prompt enter: shut ; no shut ; • Option 3: Reboot Fabric Interconnect	3.1(1e)A Resolved in 3.1(2e)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuz74973	When you use a B200 M4 server with a UCSB-MRAID12G SAS RAID controller and a CPLD firmware version earlier than version 05D, the B200 M4 server powers off unexpectedly. The OBFL displays the following log message: `[platform_power_state_irq_handler]:18:VDD_PWR_GOOD: Deasserted`	If this issue occurs, upgrade the infrastructure and server firmware to Cisco UCS Manager Release 3.1(1g) or later releases. **Note** Both infrastructure and server firmware must be upgraded. If the server firmware is upgraded to a fixed release earlier than the infrastructure firmware, do one of the following after the infrastructure firmware is upgraded to the fixed release. • Re-acknowledge the server • Decommission and then acknowledge the server This is required for the correct server firmware component to upgrade and prevent the issue.	3.1(1e)B

Defect ID	Symptom	Workaround	First Bundle Affected
CSCux68195	VMware ESXi crash (Purple Screen of Death) during certain operations while running VM FEX.	The following are possible workarounds: • Delay the upgrade to Cisco UCS Manager 3.1 until the issue is resolved • Undeploy VM FEX and instead deploy VMware. See the Software Advisory.	2.2(6c)A
CSCux52184	If you use GLC-T optics for 1G port connections on port 1-16 might not link up on UCS 6332 16UP FI	Use SFP-SX and SFP-T optics for 1G connectivity on port 1-16.	3.1(1e)A
CSCux48594	When you upgrade Cisco UCS Manager from release 2.5(2a) to 3.1, you will see DME core.	You need not take any action when you see DME core. The upgrade process will continue and complete successfully.	3.1(1e)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCux38896	After you reboot the fabric interconnect in Cisco UCS Mini, the FC port in F mode might not come up.	The following are possible workarounds: • Check with the storage vendor if the software version you are using will perform a FLOGI re-try if the first FLOGI fails. If not, ask the vendor for a software version that does FLOGI re-try and update the storage to that version (Recommended) • Flap the FC port on Cisco UCS Mini. (not recommended)	3.0(2d)A
CSCux35642	When you modify any QoS policies such as queuing or scheduling or MTU on an active system, the server discovery fails.	Reboot the FI and IOMs after any change to the QoS policy or MTU.	3.1(1e)A Resolved 3.1(1g)A
CSCuv46749	If you have Cisco UCS Blade servers B200 M4, B420 M4, B260 M4, B460 M4 in your environment, you will see random, transient critical faults with information such as 'Device reported corrupt data', when there are no data corruption.	These faults automatically clear in 30 or 40 seconds.	2.2(3g)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCux70749	When you update any driver using -ivh driver_name.rpm, kernel warnings about an unknown symbol used by an Internal Graphics Device (IGD) can be caused. This is seen for the following configurations: • Cisco UCS M142 Compute Cartridge with Intel Xeon Processor CPU 1265L v2 • Cisco UCS M1414 Compute Cartridge with Intel Xeon Processor CPU 1285L v2 • Cisco UCS M1414 Compute Cartridge with Intel Xeon Processor CPU 1285	The kernel warnings have no impact overall on IGD functionality or overall health of the operating system.	3.1(1e)M
CSCux68398	In some cases, when you perform a hardware migration for the subordinate fabric interconnect (FI-B) from UCS 6296 UP FI to UCS 6332 16UP FI, you will not be able to create FC port on the latter. This will happen if the migration is performed in the following order: 1. Launch Cisco UCS Manager GUI (Java or HTML) on a system with two UCS 6296 UP FIs. 2. Begin hardware migration for the subordinate UCS 6296 UP FI to UCS 6332-16UP FI. 3. Begin configuring FC ports using the session of Cisco UCS Manager GUI launched before migration.	To avoid this issue, do the following: • After the migration on FI-B is complete, exit the session of Cisco UCS Manager GUI. • Re-launch a new session of the same GUI to configure FC ports on UCS 6332 16UP FI.	3.1(1e)A
CSCux65310	In some cases, during blade Cisco IMC controller reboot, a chassis thermal fault may generate due to long reconnect from the IOM to the Cisco IMC.	This fault will automatically clear by itself.	3.1(1e)A Resolved in 3.1(1g)A
CSCux64421	The Cisco UCS M4308 Modular Chassis fans may run at higher than expected speeds. This occurs when a host on a cartridge fails to complete BIOS POST within the expected interval.	The fan speed returns to normal after the host completes BIOS POST, or if the host is powered off.	3.1(1e)M

Defect ID	Symptom	Workaround	First Bundle Affected
CSCup09193	When equal cost multiple uplinks (FC/FCoE) to the same adjacent switch or to different adjacent switches using which same remote domain can be reached, you will see one of the following issues: • All uplinks except one does not come up. • In case more than one uplinks come up, you will see traffic disruptions and IO timeouts.	To avoid this issue do not use equal cost multipaths at any point of time. If you need multiple individual links to the same switch, you can add all of the ports to a port-channel.	3.1(1e)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuz46574	As a result of power-up, power-down, portgroup change, or vmotion, after a VM changes its pinning, the MAC address of that VM does not get removed immediately from the MAC address table of the Cisco UCS 6332 FI to which it was earlier pinned. This happens when the uplink is port-channel.	To avoid this issue, do one of the following: • Use individual uplinks, and not port channels. • Use Fabric Failover based vNIC rather than OS teaming/failover. If the above is not possible: • Configure port groups on VMWare to have VM traffic pinned only to one side If this issue occurs, do one of the following: • Use the "clear mac address dynamic address xxxx.xxxx.xxxx" command to clear the MAC from the FI • Flap the uplink port-channel to clear stale macs on that FI	3.1(1e)A Resolved 3.1(1h)A
CSCuz69373	During Cisco UCS Manager upgrade to release 3.1(1), you will see CATERR faults due to unresponsive eCPUs. This issue happens when the eCPUs fall into diagnostic code (debug loop) after the DINT CPU input is asserted.	No known workaround.	3.1(1e)A Resolved in 3.1(1h)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuy01645	DIMM temperature readings are reported as NA when the temperature is 16 degree Celsius more than the previous reading. This results in missed temperature readings, which in turn results in Cisco UCS Manager generating thermal alerts.	This issue has no workaround.	3.1(1e)B Resolved in 3.1(1h)A
CSCuz67284	When installing the ESXi 5.5 U2 custom ISO to FlexFLash, the partedUtil fails with the following error message: “Can't have a partition outside the disk! Unable to read partition table for device."	Scrub the FlexFlash drives to install the ISO without any issues.	2.2(3d)
CSCuz46847	After IOM reset on chassis, Cisco UCS Manager may raise a fault, 'chassis major power error'. Chassis may seem to be in an inoperable state, however chassis is fully operable.	Reacknowledge the affected IOMs to resolve the issue.	3.1(1e)A
CSCuz55693	When you attempt to reset memory errors using `ucs-fi chassis/server # reset-all-memory-errors`, Cisco UCS Manager may generate a 'Managed object does not exist' error.	The command will work after you decommission the new blade and reacknowledge it.	3.1(1e)A Resolved in 3.1(1k)A
CSCuz08759	vniccfgd process crashes when downgrading VIC firmware to version 4.1(1d).	Activate the VIC adapter firmware backup image, whose version matches Cisco UCS Manger, which was installed before the downgrade.	3.1(1e)C Resolved in 3.1(1k)C

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuy35745	When upgrading or downgrading a Unified Ports Capable 3rd Generation Fabric Interconnect, the upgrade or downgrade process fails with the following error message: `"less space in /var/sysmgr"`		3.1(1e)A Resolved in 3.1(1k)A

Defect ID	Symptom	Workaround	First Bundle Affected
		To resolve the issue follow the steps below: • Load the debug plugin and get to the linux prompt on the fabric interconnect. • Delete the file "/var/sysmgr/tmp/debug". • Try the upgrade or downgrade process again. **Note** The error could happen only on Unified Ports Capable 3rd Generation Fabric Interconnect. Additionally one of the following conditions need to be satisfied: • The system is up and running for a long time. • There are lots of QoS configuration changes. • There	

Defect ID	Symptom	Workaround	First Bundle Affected
		are lots of flaps on ports 1/1-16.	
CSCux62816	When any IPMI user attribute (except IPMI user password) is modified, it blocks authentication for the IPMI user and fails all the related operations that need authentication. User is unable to login, inject UC ECC error, or perform IPMI related operations with the IPMI tool.	Set the IPMI user password again.	3.1(1e)A Resolved in 3.1(1k)A
CSCva17185	Under rare circumstances, 3 1/2-inch Seagate drives might fail when accessed after a long idle period, as the lubrication under the read head can become depleted. This problem only impacts C-series Unified Computing Systems (UCS's) with the following PID's: • UCS-HDD1TI2F212 • UCS-HDD2TI2F213 • UCS-HDD3TI2F214 • UCS-HD4T7KS3-E • UCSC-C3X60-HD4T • UCS-HD4TBK9 • UCS-HD4TBK9"	No known workaround.	2.2(3a)B

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuy52691	After upgrading Cisco UCS Manager to release 3.1(1e), changes to the maximum power allocated can prevent the blade server from powering on, with the following faults: **Description: Insufficient power available to power-on server x/y** **Affected Object: sys/chassis-x/blade-y/budget** **Name: Power Budget Power Budget Unavailable** **Description: [FSM:STAGE:RETRY:]: Check if power can be allocated to server x/y(FSM:STAGE:sam:dme:ComputeBladeDiscover:CheckPowerAvailability)** **Affected Object: sys/chassis-x/blade-yName: Fsm Sam Dme Compute Blade Discover** **Cause: Check Power Availability Failed**	If this issue occurs, do the one of the following • Change the power control policy in Service Profile to "cap" with default priority value of "5". • Change PSU power policy to N+1 from GRID.	3.1(1e)A Resolved in 3.1(2b)A
CSCva09070	Some Cisco UCS Manager pages have the `'X-Frame option is missing'` in the http message header which may result in click-jacking.	No known workaround	3.1(1e)A Resolved in 3.1(1k)
CSCva19523	When the Peer Fabric Interconnect is down, the server discovery FSM is stuck with the following message: `detect mezz cards in 1/1 (FSM-STAGE:sam:dme:ComputeBladeDiscover: NicPresencePeer)`	Bring up the Peer Fabric Interconnect.	3.1(1e)A Resolved in 3.1(1k)
CSCva61701	When the Cisco UCS FI uplinks are in the individual (" I ") state, broadcast traffic received on one interface is sent back upstream on the other interfaces.	Set the **suspend individual** value to **True** in the LACP network policy. This makes sure that the port is suspended (" S " state) instead of individual (" I" state).	3.1(1e)A Resolved in 3.1(2b)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuu24614	FC port channel gets deleted when Cisco UCS Manager perceives a speed difference between the port and port channel.	Check if the port speed matches the port channel speed, before adding the port to the port channel. In case of replacing SFP, remove the port from port channel, and then replace the SFP. **Note** Recheck to make sure that the port speed matches the port channel speed.	3.1(1e)A Resolved in 3.1(2b)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCva47085	When using VIC1340 with 2304 IOM Native 40G backplane connection (not 4x10G), LUNs disconnect or failure occurs during FC/FCOE reboot. In the VMware vmkernel log the following message may be seen: `2016-06-21T04:32:36.106Z cpu25:33191)<3>fnic : 2 :: hdr status = FCPIO_DATA_CNT_MISMATCH` In the VIC adapter log the following message may be seen: `160621-04:26:51.733255 ecom.ecom_main ecom(8:3): ox_id 41d4 rx_id 44b seq_cnt 7 seq_id 1 160621-04:26:52.066235 ecom.ecom_main ecom(8:1): fcpio_data_cnt_mismatch for exch 4202 status 1 rx_id5f7 s_stat 0x3 xmit_recvd 0x3000 burst_offset 0x3000 sgl_err 0x0 last_param 0x2800 last_seq_cnt 0x0 tot_bytes_exp 0x8000 h_seq_cnt 0x5 exch_type 0x0 s_id 0xab800 d_id 0xab800 host_tag 0x377` Non-stomped CRC is observed coming from the IOM to adapter. The following messages may be seen in the Cisco UCS Manager CLI: `connect adapter x/x/x attach-mcpdcem-macstats 0 <- check for "Rx CRC error frames not stomped" dcem-macstats 1 <- check for "Rx CRC error frames not stomped"`	If this issue occurs do one of the following: • With VIC1340 use 4x10G only, by removing the port expander. • Use the VIC1380 adapter only.	3.1(1e)A Resolved in 3.1(2b)A
CSCuy13596	During OS installation on Cisco UCS C3260 System running Cisco VIC firmware 4.1(1d) and CMC firmware 2.0(9d), the installer fails when creating partitions or writing to LUNs.	No known workaround.	3.1(1e)B 3.1(2b)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvf34463	When PXE installation is attempted on 16 or more servers at the same time, in a system with only one FI-IOM fabric link, more than two chassis with eight servers each, and more than six vNICs in a single chassis, the installation fails on a few servers.	Manually reboot the servers on which PXE installation failed.	3.1(1e)A
CSCve4771	RHEL 7.3 OS installation fails when HTML KVM is used to install the OS and mount the ISO. The following error is reported: `This program has encountered an unknown error. You may report the bug below or quit the program.`	Use Java KVM or CIMC mapped ISO to install RHEL 7.3.	3.1(1e)A

Behavior Changes and Known Limitations

UCS 6300 Series Fabric Interconnect ASIC Limitation with Passive Cables

UCS 6300 Series FIs support passive cables, except on the uplink ports. The ASIC on the FI does not support auto-negotiation (CSCvc98464), which is why only active cables are recommended for use on uplink ports.

This limitation also applies when connecting non-uplink ports to upstream switch ports that do not support auto-negotiation. When using passive cables, the link may not work because the 6300 Series FI uses auto-negotiation, and the peer switch port does not support it. You cannot disable auto-negotiation on the 6300 Series FI, which is why Cisco recommends that you use active cables in such a scenario.

Cisco UCS Manager GUI

Beginning with Cisco UCS Manager Release 3.1(3a), the Cisco UCS Manager GUI is no longer available as a Java-based application.

HTML5 KVM Support

Prior to Cisco UCS Manager Release 3.1(3), all platforms supported the Java KVM client only. Cisco UCS Manager Release 3.1(3) introduces the HTML5 KVM client. HTML5 KVM is only for M3 and later servers that run on Cisco UCS Manager Release 3.1(3). M3 rack servers support HTML5 KVM in Cisco UCS Manager-managed mode only.

Some older platforms do not support the HTML5 KVM client. For these platforms, Cisco UCS Manager does not display the **Launch Java KVM Console** option, and directly launches the Java KVM console.

A few KVM features are not supported on the HTML5 KVM client. To use these features, or to use the Java KVM client on platforms that support the HTML5 KVM client, check the **Launch Java KVM Console** checkbox and then click OK.

Cisco UCS Manager Software Activation through Auto Install

CSCuy52691—In Cisco UCS Manager Releases 3.1(1l), 3.1(2b), 3.1(2c), and 3.1(2e), activating the Cisco UCS Manager software through Auto Install fails if the power policy is configured with **Redundancy** set to **Grid** and **Power Capping** set to **No Cap**.

CSCvc85609—In Cisco UCS Manager releases earlier than Cisco UCS Manager Release 3.1(2b) and later than 3.1(2e), activating the Cisco UCS Manager software through Auto Install does not fail based on the configured power policy.

Host Firmware Package Policy

The global-default host firmware package policy includes all components. However, from Cisco UCS Release 3.1(1g), if you create a new custom host firmware package policy, the local disk component is automatically excluded.

Key Ring Modulus Size Support

CSCuo28600—Cisco UCS Manager Release 3.1 does not support key rings that have modulus size less than 2048 bits. Before you upgrade to Cisco UCS Manager Release 3.1(1), ensure that the key ring in use has a modulus size of 2048 bits or higher. For example, if the key ring modulus size is set to 1024, change the value to 2048 or higher. For specific guidelines for firmware upgrade, see the Firmware Upgrade to Cisco UCS Manager Release 3.1 section of the Cisco UCS Manager Firmware Management Guide.

The following caveat is a known limitation in Release 3.1(3a):

Table 26: Known limitations in Release 3.1(3a)

Defect ID	Platform	Symptom	Workaround
CSCvd79583	All	Systems under heavy stress, or targets that are slow to respond result in the following event IDs getting logged on Windows 2012 R2 and Windows 2016. • Event ID 153—When the fNIC driver times out the I/O. • Event ID 129—When the storport driver ultimately times out the I/O.	Use Cisco UCS Manager to change the Windows default I/O timeout from 5 seconds to 25 seconds.

The following caveat is a known limitation in Release 3.1(2b):

Table 27: Known limitations in Release 3.1(2b)

Defect ID	Platform	Symptom	Workaround
CSCuz76448	All	In Cisco UCS 3260 systems, in rare cases, when RAID is configured with LSI Software RAID, and Linux install is attempted using an Intel driver, system boot may become unresponsive at the LSI Software RAID option ROM due to the erroneous install attempt.	

Defect ID	Platform	Symptom	Workaround

			If this issue occurs, do one of the following:
			• Remove the drives, boot to the LSI Software RAID Option ROM Ctrl+M menu, insert drives, and clear the configuration.
			• Move the drives to a MegaRAID system, delete the configuration on the drives, move back to the original system, and use with LSI Software RAID
			• Disable LSI Software RAID option ROM from Cisco IMC (tokens), boot to live CD/USB, remove the configuration, and enable the option ROM again.
			• Replace drives.
			• Try the following to wipe out the DDF on problematic SSDs:
			  • Swap the drives and go to Ctrl+M, and clear the configuration. In case there is no VD, create R1 using the same drives and clear the configuration.
			  • Remove one of the drives and go to Ctrl+M, and insert the other corrupted drive. Create R1 using the same drives, and clear the configuration.
			• Do the following:
			  1. Remove both the corrupted drives.
			  2. Insert any one drive.
			  3. Go to Ctrl+M.
			  4. Remove and insert both the corrupted drives.
			  5. Clear the configuration. In case there is no VD, create R1 using the same drives and

Defect ID	Platform	Symptom	Workaround
			clear the configuration.

The following caveat is a known limitation in Release 3.1(1h):

Table 28: Known limitations in Release 3.1(1h)

Defect ID	Platform	Symptom	Workaround
CSCuz54473	All	When you create an adapter policy in Cisco UCS Manager for Microsoft SMB Direct with RoCE Ethernet vNICs , you can set the number of queue pairs per adapter for between 1 and 8192. However, you cannot set this value to 2. When you execute the following command in Windows PowerShell with the number of queue pairs set to 2, a blank value for MaxQueuePairCount will be seen. **<Cm dbold>Get-NetAdapterRdma | fl * | findstr "MaxQueuePairCount"<noCmdBold>**	When this issue occurs, change the Queue Pairs value to 4. This value includes the two Queue Pairs reserved by the Windows enic driver. After you set the Queue Pairs value to 4, run the following command in Windows PowerShell. You will see the value for MaxQueuePairCount as 2. **<Cmdbold>Get-NetAdapterRdma | fl * | findstr "MaxQueuePairCount"<noCmdBold>** **<CmdArg>MaxQueuePairCount : 2<noCmdArg>**

The following caveats are known limitations in Release 3.1(1e):

Table 29: Known limitations in Release 3.1(1e)

Defect ID	Platform	Symptom	Workaround
CSCut76096	All	In Cisco UCS Manager the GUI task and the CLI command to reset both correctable and uncorrectable error counts on a per DIMM basis resets the errors in the **UCSM count** only. You can also see the following: • The count on Cisco IMC remains unchanged. In Cisco IMC, the health LED might continue to show the errors • If DIMM blacklisting is enabled, it continues to map the DIMM with the uncorrectable errors out of the memory configuration. **Important** Beginning with Cisco UCS Manager, Release 3.1, the GUI task and the CLI command to reset memory errors on a per DIMM basis has been replaced with per server reset-all-memory-errors.	You can use **reset-all-memory-errors** command to reset the errors in Cisco UCS Manager and Cisco IMC for all the DIMMs on a given server.