Release Notes for Cisco UCS Manager, Release 3.2

First Published: 2017-08-17

Last Modified: 2020-09-22

Cisco UCS Manager

Cisco UCS™ Manager, Release 3.2 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 3.2. This document also includes the following:

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

Upgrading directly to Cisco UCS Manager 3.2(x) is supported from Release 2.2(8) and later releases. For UCS Mini, upgrading directly to Cisco UCS Manager Release 3.2(x) is supported from Release 3.0(1) and later releases. See the *Cisco UCS Manager Firmware Management Guide, Release 3.2* section Firmware Upgrade to Cisco UCS Manager Release 3.2 for details.

Revision History

Release	Date	Description
3.2(1d)	August 17, 2017	Created release notes for Cisco UCS Manager Release 3.2(1d).
	August 23, 2017	Updated release notes to include supported CPUs and Memory for M5 servers.
	September 12, 2017	Updated the *Cisco UCS Manager and Cisco UCS C-Series Release Compatibility Matrix for C-Series Rack-Mount Servers* section Added CSCvf34463 to the list of Open Caveats.
	May 30, 2018	Updated the Open Caveats for Release 3.2(1d) with CSCvj59299, CSCvj59301, CSCvj54880, CSCvj54847, CSCvj54187, CSCvj59266, and their Software Advisory.
	February 26, 2019	Removed CSCvf32853 from the list of Resolved Caveats.
3.2(2b)	October 09, 2017	Updated release notes for Cisco UCS Manager Release 3.2(2b).
	October 19, 2017	Added CSCvd72179, CSCvf27392 and CSCvf16289 to the list of security fixes.
	November 1, 2017	Updated the minimum release for direct upgrade to Cisco UCS Manager Release 3.2(x) to Release 2.2(8)
	August 14, 2018	Updated the Behavior Changes and Known Limitations section for vNIC and vHBA configuration behavior.
	October 5, 2018	Clarified the vNIC and vHBA configuration behavior in the Behavior Changes and Known Limitations section.

Release	Date	Description
3.2(2c)	November 29, 2017	Updated release notes for Cisco UCS Manager Release 3.2(2c).
	December 02, 2017	Added Nvidia M60 GPUs to the list of new hardware for Cisco UCS Manager Release 3.2(2c).
3.2(2d)	December 18, 2017	Updated release notes for Cisco UCS Manager Release 3.2(2d).
	January 22, 2018	Added the Software Advisory for CSCvh31577 and CSCvg97982.
3.2(2f)	March 21, 2018	Updated release notes for Cisco UCS Manager Release 3.2(2f).
3.2(3a)	March 21, 2018	Updated release notes for Cisco UCS Manager Release 3.2(3a).
	May 15, 2018	Added the Software Advisory for CSCvj32984
	May 30, 2018	Added the Software Deferral Notice for CSCvj50398
	February 26, 2019	Updated the Capability Catalog for Cisco UCS Manager Release 3.2(3a) with UCS B200 M5 CPUs.
	June 10, 2021	Added the deprecated third-party adapters list.
3.2(3b)	May 14, 2018	Updated release notes for Cisco UCS Manager Release 3.2(3b).
	May 15, 2018	Added the Software Advisory for CSCvj32984
	May 30, 2018	Added the Software Deferral Notice for CSCvj50398
3.2(3d)	May 30, 2018	Updated release notes for Cisco UCS Manager Release 3.2(3d).
3.2(3e)	June 25, 2018	Updated release notes for Cisco UCS Manager Release 3.2(3e).

Release	Date	Description
3.2(3g)	July 20, 2018	Updated release notes for Cisco UCS Manager Release 3.2(3g).
	August 27, 2018	Added the L1 Terminal Fault caveats — CSCvm02934, CSCvm03356, CSCvm03351, and CSCvm03339 — to the list of Security Fixes.
3.2(3h)	September 10, 2018	Updated release notes for Cisco UCS Manager Release 3.2(3h).
3.2(3i)	November 05, 2018	Updated release notes for Cisco UCS Manager Release 3.2(3i).
3.2(3j)	January 17, 2019	Updated release notes for Cisco UCS Manager Release 3.2(3j).
3.2(3k)	April 18, 2019	Updated release notes for Cisco UCS Manager Release 3.2(3k).
	June 3, 2019	Added a known limitation - UCS 6300 Series Fabric Interconnect ASIC Limitation with Passive Cables.
3.2(3l)	September 17, 2019	Updated release notes for Cisco UCS Manager Release 3.2(3l).
3.2(3n)	February 13, 2020	Updated release notes for Cisco UCS Manager Release 3.2(3n).
	February 14, 2020	Added CSCvr37150 and CSCvr15082 to the list of Security Fixes.
3.2(3o)	June 12, 2020	Updated release notes for Cisco UCS Manager Release 3.2(3o).
3.2(3p)	September 22, 2020	Updated release notes for Cisco UCS Manager Release 3.2(3p).

Top Reasons to Move to Cisco UCS Manager Release 3.2

Here are the top reasons to move to Cisco UCS Manager Release 3.2:

- Support for UCS and Hyperflex M5 generation servers and numerous additional peripherals.
- Support for Cisco Intersight through the Device Connector.

- Ability to stage firmware through **Prepare for Update** while the systems are online, and without a maintenance window. Activating the firmware, which may require a reboot, is done much more quickly reducing the downtime during the maintenance window.
- Cisco UCS Manager Release 3.2(3) is the patch point for the Cisco UCS Manager 3.2 release train.

New Features in Release 3.2

Cisco UCS Manager, Release 3.2 is a unified software release for all supported UCS hardware platforms.

New Hardware Features

- New Hardware in Release 3.2(3p) — None
- New Hardware in Release 3.2(3o) — None
- New Hardware in Release 3.2(3n) — None
- New Hardware in Release 3.2(3l) — None
- New Hardware in Release 3.2(3k) — None
- New Hardware in Release 3.2(3j) — None
- New Hardware in Release 3.2(3i) — None
- New Hardware in Release 3.2(3h) — None
- New Hardware in Release 3.2(3g) — None
- New Hardware in Release 3.2(3e) — None
- New Hardware in Release 3.2(3d) — None
- New Hardware in Release 3.2(3b) — None
- New Hardware in Release 3.2(3a), on page 6
- New Hardware in Release 3.2(2f) — None
- New Hardware in Release 3.2(2d) — None
- New Hardware in Release 3.2(2c), on page 8
- New Hardware in Release 3.2(2b), on page 9
- New Hardware in Release 3.2(1d), on page 10

New Software Features

- New Software Features in Release 3.2(3p)
- New Software Features in Release 3.2(3o) — None
- New Software Features in Release 3.2(3n) — None
- New Software Features in Release 3.2(3l) — None
- New Software Features in Release 3.2(3k) — None

- New Software Features in Release 3.2(3j) — None
- New Software Features in Release 3.2(3i) — None
- New Software Features in Release 3.2(3h) — None
- New Software Features in Release 3.2(3g) — None
- New Software Features in Release 3.2(3e) — None
- New Software Features in Release 3.2(3d) — None
- New Software Features in Release 3.2(3b) — None
- New Software Features in Release 3.2(3a), on page 12
- New Software Features in Release 3.2(2f) — None
- New Software Features in Release 3.2(2d) — None
- New Software Features in Release 3.2(2c) — None
- New Software Features in Release 3.2(2b), on page 13
- New Software Features in Release 3.2(1d), on page 13

New Hardware in Release 3.2(3a)

M5 Servers

- Support for the UCS-S3260-M5SRB server
- Support for the following NVMe-optimized M5 servers:
  - UCSC-C220-M5SN—The PCIe MSwitch is placed in the dedicated MRAID slot for UCS C220 M5 servers. This setup supports up to 10 NVMe drives. The first two drives are direct-attached through the riser. The remaining eight drives are connected and managed by the MSwitch. This setup does not support any SAS/SATA drive combinations.
  - UCSC-C240-M5SN—The PCIe MSwitch is placed in the riser-2 at slot-4 for UCS C240 M5 servers. The servers support up to 24 drives. Slots 1-8 are the NVMe drives connected and managed by the MSwitch. The servers also support up to two NVMe drives in the rear and are direct-attached through the riser. This setup supports SAS/SATA combination with the SAS/SATA drives from slots 9-24. These drives are managed by the SAS controller placed in the dedicated MRAID PCIe slot.
  - UCS-C480-M5—UCS C480 M5 servers support up to three front NVMe drive cages, each supporting up to eight NVMe drives. Each cage has an interposer card, which contains the MSwitch. Each server can support up to 24 NVMe drives (3 NVMe drive cages x 8 NVMe drives). The servers also support a rear PCIe Aux drive cage, which can contain up to eight NVMe drives managed by an MSwitch placed in PCIe slot-10.

    This setup does not support:

    - a combination of NVMe drive cages and HDD drive cages
    - a combination of the Cisco 12G 9460-8i RAID controller and NVMe drive cages, irrespective of the rear Auxiliary drive cage

Note The UCS C480 M5 PID remains same as in earlier release.

Peripherals

- Support for the Cisco 12G 9460-8i RAID controller with 2GB cache (UCSC-SAS9460-8I) for UCS C480 M5 rack-mount servers.

  Support for UCS C480 M5 (UCSC-C480-8AUX) Auxiliary Drive Modules for the Cisco 12G 9460-8i RAID controller.

- Support for the following new NVMe SSD drives on UCS S3260 M5 servers:
  - UCS S3260 500GB NVMe for M5 Server Node/SIOC (UCS-S3260-NVG25)
  - UCS S3260 1TB NVMe for M5 Server Node/SIOC (UCS-S3260-NVG210)
  - UCS S3260 2TB NVMe for M5 Server Node/SIOC (UCS-S3260-NVG220)

- Support for the following new NVMe SSD drives on all M5 servers:
  - HGST SN200 1.6TB 2.5 in SSD (UCSC-NVMEHW-H1600)
  - HGST SN200 3.2TB 2.5 in SSD (UCSC-NVMEHW-H3200)
  - HGST SN200 6.4TB 2.5 in SSD (UCSC-NVMEHW-H6400)
  - HGST SN200 7.7TB 2.5 in SSD KNCCD101 (UCSC-NVMEHW-H7680)
  - HGST SN200 800GB 2.5 in SSD (UCSC-NVMEHW-H800)

- Support for the following new NVMe SSD drives on NVMe-optimized M5 servers:
  - Cisco 2.5" 375GB Intel Xpoint BRAND NVMe Extreme Perf (UCSC-NVMEXP-I375) - Supported only on C220 M5
  - Cisco 2.5" 750GB Intel Xpoint BRAND NVMe Extreme Perf. (UCSC-NVMEXP-I750) - Supported only on C220 M5
  - Cisco 2.5" 1.6TB Intel P4600 NVMe High Perf High Endurance (UCSB-NVMEHW-I1600)
  - Cisco 2.5" 2TB Intel P4600 NVMe High Perf High Endurance (UCSB-NVMEHW-I2000)
  - Cisco 2.5" 3.2TB Intel P4600 NVMe High Perf High Endurance (UCSB-NVMEHW-I3200)
  - Cisco 2.5" 1TB Intel P4500 NVMe High Perf Value Endurance (UCSB-NVMEHW-I1000)
  - Cisco 2.5" 2TB Intel P4500 NVMe High Perf Value Endurance (UCSB-NVMEHW-I2TBV)
  - Cisco 2.5" 4TB Intel P4500 NVMe High Perf Value Endurance (UCSB-NVMEHW-I4000)
  - Cisco 2.5" 500GB Intel P4501 NVMe Med. Perf. Value Endurance (UCSB-NVMELW-I500)
  - Cisco 2.5" 1TB Intel P4501 NVMe Med. Perf. Value Endurance (UCSB-NVMELW-I1000)
  - Cisco 2.5" 2TB Intel P4501 NVMe Med. Perf. Value Endurance (UCSB-NVMELW-I2000)

- Support for the following PCIe cards on the IOE for a server node with UCS S3260 M5 servers:
  - Intel X550 dual-port 10GBase-T (UCSC-PCIE-ID10GC)
  - Qlogic QLE2692 dual-port 16G Fiber Channel HBA (UCSC-PCIE-QD16GF
- Support for the following MSwitch card in NVMe optimized M5 servers:
  - UCS-C480-M5 HDD Ext NVMe Card (UCSC-C480-8NVME)—Front NVMe drive cage with an attached interposer card containing the PCIe MSwitch. Each server supports up to three front NVMe drive cages and each cage supports up to 8 NVMe drives. Each server can support up to 24 NVMe drives (3 NVMe drive cages x 8 NVMe drives).
  - UCS-C480-M5 PCIe NVMe Switch Card (UCSC-NVME-SC)—PCIe MSwitch card to support up to eight NVMe drives in the rear auxiliary drive cage inserted in PCIe slot 10.

    Note Cisco UCS-C480-M5 servers support a maximum of 32 NVMe drives (24 NVMe drives in the front + 8 NVMe drives in the rear auxiliary drive cage)

  - UCSC-C220-M5SN and UCSC-C240-M5SN do not have separate MSwitch PIDs. MSwitch cards for these servers are part of the corresponding NVMe optimized server.
- Support for the following NVIDIA GPUs:
  - P4 GPUs with C220 M5 and C240 M5 servers
  - V100 GPUs with C240 M5, C480 M5 servers
- Support for the following Intel adapter with UCS M5 servers:
  - Intel XL710 adapter (UCSC-PCIE-ID40GF) (not supported on S3260 M5)
  - Intel XXV710-DA2 adapter (XXV710-DA2) (not supported on S3260 M5)
  - Intel X710-DA4 adapter (UCSC-PCIE-IQ10GF) (not supported on S3260 M5)
  - Intel X710-DA2 adapter (UCSC-PCIE-ID10GF) (not supported on S3260 M5)
  - Intel X710-T4 adapter (X710-T4)
  - Intel X550-T2 adapter (UCSC-PCIE-ID10GC)
  - Intel X520 dual port adapter (N2XX-AIPCI01)
- Support for the following storage controllers:
  - UCS S3260 Dual Pass Through (UCS-S3260-DHBA)
  - UCS S3260 Dual RAID (UCS-S3260-DRAID)

New Hardware in Release 3.2(2c)

Peripherals

Support for NVIDIA Tesla M60 GPUs.

New Hardware in Release 3.2(2b)

M5 Servers

- Support for the UCS B480 M5 blade server

  Note Only Cisco UCS VIC 1340 and VIC 1380 adapters are supported on UCS B480 M5 servers.

- Support for the UCS C480 M5 rack-mount servers

  Note Only Cisco UCS VIC 1385 is supported on UCS C480 M5 servers.

Peripherals

- Support for the following new NVMe devices with relevant UCS M4 and M5 servers:
  - Cisco 2.5" U.2 800GB HGST SN200 NVMe High Perf. High Endurance:
    - For UCS M4 Servers - UCSC-NVMEM4-H800
    - For UCS M5 Severs - UCSC-NVMEHW-H800
  - Cisco 2.5" U.2 1.6 TB HGST SN200 NVMe High Perf. High Endurance:
    - For UCS M4 Servers - UCSC-NVMEM4-H1600
    - For UCS M5 Severs - UCSC-NVMEHW-H1600
  - Cisco HHHL AIC 6.4TB HGST SN260 NVMe Extreme Perf High Endurance for UCS M4 and M5 servers (UCSC-NVME-H64003)
  - Cisco HHHL AIC 7.7TB HGST SN260 NVMe Extreme Perf High Endurance for UCS M4 and M5 servers (UCSC-NVME-H76801)
  - Cisco HHHL AIC 3.2TB SN260 NVMe Extreme Perf High Endurance for UCS M4 and M5 servers (UCSC-NVME-H32003)
- Support for NVIDIA P4 GPUs with UCS C240 M5 servers
- Support for the following Qlogic adapters with UCS M5 servers:
  - QLogic QL41212H 25GbE (UCSC-PCIE-QD25GF)
  - QLogic QL45412H 40GbE (UCSC-PCIE-QD40GF)
- Support for the following Intel adapter with UCS M5 servers:
  - Intel X710-T4 (UCSC-PCIE-IQ10GC)
- Azure stack support on the following adapters:
  - QLogic 40G card (UCSC-PCIE-QD40GF)

- Cisco HHHL AIC 3.2TB SN260 (UCSC-NVME-H32003)

New Hardware in Release 3.2(1d)

M5 Servers

- Support for the UCS B200 M5 blade server

Note Only Cisco UCS VIC 1340 and VIC 1380 adapters are supported on UCS B200 M5 servers.

- Support for UCS C220 M5 and UCS C240 M5 rack-mount servers

Note Only Cisco UCS VIC 1385 and VIC 1387 adapters are supported on UCS C220 M5 and UCS C240 M5 servers.

- Enablement for Cisco HX220 M5, HX240 M5, HXAF 220 M5, HXAF 240 M5 servers
- Support for UCS M5 servers on Cisco UCS 6200 Series, 6300 Series, and 6324 fabric interconnects
- Support for UCS M5 servers with UCS IOMs 2204, 2208, and 2304
- Support for UCS FEX-based connectivity to UCS M5 rack-mount servers.

Peripherals

- Support for the following new NVMe devices with relevant UCS M5 servers:
  - Cisco 2.5" U.2 800GB HGST SN200 NVMe High Perf. High Endurance (UCSC-NVMEHW-H800)
  - Cisco 2.5" U.2 1.6 TB HGST SN200 NVMe High Perf. High Endurance (UCSC-NVMEHW-H1600)
  - Cisco 2.5" U.2 3.2 TB HGST SN200 NVMe High Perf. High Endurance (UCSC-NVMEHW-H3200)
  - Cisco 2.5" U.2 6.4 TB HGST SN200 NVMe High Perf. High Endurance (UCSC-NVMEHW-H6400)
  - Cisco 2.5" U.2 7.7 TB HGST SN200 NVMe High Perf. High Endurance (UCSC-NVMEHW-H7680)
  - Cisco 3.5" LFF 800GB HGST SN200 NVMe High Perf. High Endurance (UCSC-NVMEHY-H800)
  - Cisco 3.5" LFF 1.6TB HGST SN200 NVMe High Perf. High Endurance (UCSC-NVMEHY-H1600)
  - Cisco 3.5" LFF 3.2TB HGST SN200 NVMe High Perf. High Endurance (UCSC-NVMEHY-H3200)
  - Cisco HHHL AIC 1.6TB HGST SN250 NVMe Extreme Perf High Endurance (UCSC-NVME-H16003)
  - Cisco HHHL AIC 3.2TB HGST SN250 NVMe Extreme Perf High Endurance (UCSC-NVME-H32003)
  - Cisco HHHL AIC 3.8TB HGST SN250 NVMe Extreme Perf High Endurance (UCSC-NVME-H38401)

  - Cisco HHHL AIC 6.4TB HGST SN250 NVMe Extreme Perf High Endurance (UCSC-NVME-H64003)
  - Cisco HHHL AIC 7.7TB HGST SN250 NVMe Extreme Perf High Endurance (UCSC-NVME-H76801)

- Support for the following NVIDIA P6 GPUs with UCS B200 M5 blade servers:
  - UCSB-GPU-P6-F
  - UCSB-GPU-P6-R

- Support for the following NVIDIA P40 GPU with UCS C240 M5 rack-mount servers:
  - UCSC-GPU-P40

- Support for the following Qlogic adapters with UCS C220 M5 and UCS C240 M5 rack-mount servers:
  - Qlogic QLE2692 dual-port 16G Fibre Channel HBA (UCSC-PCIE-QD16GF)
  - Qlogic QLE2672-CSC, 16Gb Fibre Channel with SR Optics HBA (UCSC-PCIE-Q2672)
  - Qlogic QLE2742 dual-port 32G Fibre Channel HBA (UCSC-PCIE-QD32GF)

- Support for the following Emulex adapters with UCS C220 M5 and UCS C240 M5 rack-mount servers:
  - Emulex LPe32000-M2 single-port 32G HBA (UCSC-PCIE-BS32GF)
  - Emulex LPe32000-M2 dual-port 32G HBA (UCSC-PCIE-BD32GF)
  - Emulex LPe16002-M6 16G FC rack HBA (UCSC-PCIE-E16002)

- Support for SD storage modules (UCS-MSTOR-SD) on UCS M5 servers
- Support for the following SD cards with UCS-MSTOR-SD:
  - UCS-SD-32G-S
  - UCS-SD-64G-S
  - UCS-SD-128G

- Support for M.2 SATA storage modules (UCS-MSTOR-M2) on UCS M5 servers
- Support for the following M.2 SATA drives with UCS-MSTOR-M2:
  - 240GB M.2 6G SATA SSD (UCS-M2-240GB)
  - 960GB M.2 6G SATA SSD (UCS-M2-960GB)

- Support for the following RAID controllers:
  - Cisco 12G Modular Raid controller with 2GB cache (max 16 drives) (UCSC-RAID-M5) - For UCS C220 M5 and C240 M5 rack-mount servers.
  - Cisco 12G Modular Raid controller with 4GB cache (max 26 drives) (UCSC-RAID-M5HD) - For UCS C240 M5 rack-mount servers

- Cisco 12G Modular SAS HBA (max 16 drives) (UCSC-SAS-M5) - For UCS C220 M5 and C240 M5 rack-mount servers.
- Cisco 12G Modular SAS HBA (max 26 drives) (UCSC-SAS-M5HD) - For UCS C240 M5 rack-mount servers.
- LSI MegaRAID SAS 3108 (UCSC-MRAID12G) - For UCS C220 M5 rack-mount servers (C220-M5L).

New Software Features in Release 3.2(3a)

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

Feature Enhancements

- Support for UCS S3260 M5 Servers—Cisco UCS S3260 M5 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. Each server node has two M5 CPUs, which are based on the latest architecture from Intel and powered by the new Intel Xeon Processor Scalable family. The Cisco UCS S3260 M5 system can be operated in a standalone environment or as part of the Cisco Unified Computing System with Cisco UCS Manager integration. *Cisco UCS C3260 Server Integration with Cisco UCS Manager*, Release 3.2 provides detailed information.
- Support for NVMe-optimized servers—Cisco UCS Manager extends support for NVMe optimized Cisco UCS C220 M5, C240 M5, and C480 M5 servers.
- Single Path support for UCS S3260 Dual Pass Through (UCS-S3260-DHBA) controller—In Cisco UCS S3260 M5 servers, Cisco UCS Manager enables single path access to disks by configuring a single DiskPort per disk slot. Setting single path configuration ensures that the server discovers the disk drive only through a single drive path chosen in the configuration.
- S3260 Chassis Firmware Update through Auto-Install—Beginning with Cisco UCS Manager Release 3.2(3), the firmware of Cisco UCS S3260 chassis components can be upgraded in a single step by using Auto Install.
- Prepare for Update—Cisco UCS Manager Release 3.2(3) introduces the ability to update or stage the firmware of infrastructure, server components, and S3260 chassis simultaneously, and keep it independent of the activation process. Because staging firmware does not involve rebooting any endpoints, this ability allows staging of the firmware on all endpoints without waiting for a maintenance window. Consequently, the time taken to complete the Auto Install process no longer includes the time taken to stage the firmware of all endpoints. Thus, it significantly reduces the downtime required for maintenance.

  This ability to stage firmware outside of the Auto Install process does not change the legacy ability of Auto Install to stage and activate the firmware of components.
- Customer Certificate for KVM Usage— This Cisco UCS Manager release enables the KVM certificate to be changed only on Cisco UCS M5 servers.
- 6G-12G Mixed Mode—**6G-12G Mixed Mode** is available for **SAS Expander Configuration Policy**. This mode enables the connection management to intelligently monitor and shift between 6G and 12G speeds, based on availability.
- Parallel Disk Upgrade for HBA Controllers—Beginning with Cisco UCS Manager Release 3.2(3), firmware for disks attached to IT/HBA controllers is updated in parallel. This is applicable for UCS M4 and M5 rack-mount servers only.

- Support for Integrated UCS C-Series M5 Server Diagnostics—The Cisco UCS Manager diagnostics tool enables you to diagnose hardware components, such as memory and CPU on UCS C-Series M5 servers using PMEM2 memory test.
- PXE IPV6 Support—Cisco UCS Manager boot policy now has an IPV6 enable option for each PXE boot device interface. PXE IPV6 support is only for UCS M5 blade and rack servers, and can be enabled in the UEFI boot policy.
- Scale Optimization for Server Discovery—In a setup with 2K VLANs, 19 chassis, and 12 rack servers, server discovery was taking 2 hours after changing the chassis policy from portchannel to none. This delay has now been significantly reduced.
- Consistent Device Naming (CDN) support for ESXi—CDN support has been expanded to include ESXi 6.7.

New Software Features in Release 3.2(3p)

ADDDC RAS Changes

- Adaptive Double Device Data Correction (ADDDC) is a memory RAS feature that enables dynamic mapping of failing DRAM by monitoring corrected errors and taking action before uncorrected errors can occur and cause an outage. It is now enabled by default.

  After ADDDC sparing remaps a memory region, the system could incur marginal memory latency and bandwidth penalties on memory bandwidth intense workloads that target the impacted region. Cisco recommends scheduling proactive maintenance to replace a failed DIMM after an ADDDC RAS fault is reported.

New Software Features in Release 3.2(2b)

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

Feature Enhancements

- Support for UCS B480 and C480 M5 Servers—Based on the latest architecture from Intel and powered by the new Intel Xeon Processor Scalable family, the M5 four-socket servers offer improved processing performance (up to 28-cores per socket) and faster memory (up to 2666MHz). The servers also bring improved memory, storage and GPU density, including more NVMe options per server, support for more GPUs, and an M.2 option. Cisco UCS Manager extends support for all existing features on the following Cisco UCS B-Series and C-Series M5 servers unless specifically noted:
  - C480 M5 Server
  - B480 M5 Server
- Power Node Manager Support for Blade Servers—In this release, the chassis dynamic power rebalance mechanism is enabled by default. This mechanism continuously monitors the power usage of the blade servers and adjusts the power allocation accordingly.
- Support for 1000 IGMP Snooping Groups—Cisco UCS Manager now supports 1000 IGMP Snooping Groups.

New Software Features in Release 3.2(1d)

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

Feature Enhancements

- Support for UCS M5 Servers—Based on the latest architecture from Intel and powered by the new Intel Xeon Processor Scalable family, the M5 dual-socket servers offer improved processing performance (up to 28-cores per socket) and faster memory (up to 2666MHz). The servers also bring improved memory, storage and GPU density, including more NVMe options per server, support for more GPUs, and an M.2 option. Cisco UCS Manager extends support for all existing features on the following Cisco UCS B- and C-Series M5 servers unless specifically noted:
    - B200 M5
    - C220 M5
    - C240 M5
- Device Connector— Device connector connects Cisco UCS Manager to Cisco Intersight, the cloud-hosted server management system, and is enabled by default. It enables Cisco UCS Manager to be managed and monitored through Cisco Intersight.

  The device connector makes connections to the cloud when Cisco UCS Manager is being upgraded to Release 3.2.
- Support for Embedded Software RAID—This release extends the existing embedded software RAID support for UCS M5 servers.
- Warm Removal of NVMe Drives—Cisco UCS Manager now supports warm removal of NVMe drives for blade and rack servers.
- NVMe Boot for M5 Servers—Cisco UCS Manager provides an option of adding an NVMe device to the boot policy for UCS M5 blade and rack servers.
- HTML5 KVM Folder Mapping—This release introduces HTML5 KVM folder mapping support. Folder mapping provides external file access to the KVM console through the HTML5 KVM interface for remote system updates. This feature is available for B-Series and C-Series servers on systems running Google Chrome version 57 and higher.
- Support for UCS Firmware Package MD5 Checksum—Cisco UCS Manager Release 3.2 introduces support for MD5 checksum of firmware packages. After downloading the firmware package, you can use this checksum to validate that the package downloaded correctly.
- Custom GUI Inactivity Time Out Value—You can now set the GUI inactivity timeout to log users out of Cisco UCS Manager if they have been inactive for a specified period of time.

Deprecated Hardware and Software in Cisco UCS Manager Release 3.2

Cisco UCS Manager Release 3.2 does not support hardware or software that was deprecated in Cisco UCS Manager Release 3.1(x).

The Release Notes for Cisco UCS Manager, Release 3.1 lists the hardware and software deprecated in Release 3.1(x).

Deprecated Software in Release 3.2

VM-FEX—Cisco UCS Manager Release 3.2 includes support for the SR-IOV implementation of the VM-FEX feature. However, non SR-IOV implementations of the VM-FEX feature, for example, VM-FEX deployments of VMware vSphere Hypervisor, are not supported on Cisco UCS M5 servers.

Deprecated Hardware in Release 3.2(3a)

Starting with Cisco UCS Manager Release 3.2(3a), the Cisco UCS Manager does not support the third-party adapters (vNIC & vHBA) listed in the following table. However, the adapter support is limited to inventory and firmware management.

Table 1: Deprecated hardware from Release 3.2(3a)

Hardware Type	Product
Adapters	Intel X550 dual-port 10GBase-T (UCSC-PCIE-ID10GC)
	Intel X520 dual port 10G SFP (N2XX-AIPCI01)
	Emulex dual port 10GBase-T (UCSC-PCIE-BTG)
	Emulex dual port 10G SFP (UCSC-PCIE-B3SFP)
	Emulex dual port 10G SFP (UCSC-PCIE-E14102B)
	QLogic QLE8442 10GBase-T network adapter (UCSC-PCIE-QNICSFP)
	QLogic QLE8442 10Gb Dual port 10GBaseT network adapter (UCSC-PCIE-QNICBT)

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 3.2(1) is integrated with C-Series Standalone Release 3.1(1) for the M5 servers and Release 3.0(3) for all M3 and M4 servers. Hence, it supports all the M5, M4 and M3 servers supported by C-Series Standalone releases. The Internal Dependencies, on page 19 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 2: Cisco UCS Manager and C-Series Software releases for C-Series Servers

Cisco UCS Manager Release	C-Series Standalone Releases Included	C-Series Servers Supported by the C-Series Standalone Releases
3.2(3)	3.1(3)	C220 M5, C240 M5, C480 M5, S3260 M5 only
	3.0(4)	All M3/M4

Cisco UCS Manager Release	C-Series Standalone Releases Included	C-Series Servers Supported by the C-Series Standalone Releases
3.2(2)	3.1(2)	C220 M5, C240 M5, C480 M5 only
	3.0(3)	All M3/M4
3.2(1)	3.1(1)	C220 M5, C240 M5 only
	3.0(3)	All M3/M4
3.1(3)	3.0(3)	All M3/M4
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

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.

Beginning with Cisco UCS Manager Release 3.2(1d), the KVM Launch Manager GUI is no longer available as a Java-based application. The KVM GUI is still available as a Java-based application, and is required for KVM sessions on servers that do not support the HTML5 KVM GUI.

Cisco UCS Central Integration

Cisco UCS Manager Release 3.2 can only be registered with Cisco UCS Central, Release 2.0(1b) or higher.

Supported Operating Systems

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

Supported Web Browsers

Cisco UCS Manager GUI	Web Browsers
HTML5	Microsoft Internet Explorer 11 or higher Mozilla Firefox 45 or higher Google Chrome 57 or higher Apple Safari version 9 or higher Opera version 35 or higher

Network Requirements

For using the device connector feature, you must configure HTTPS proxy settings. The *Cisco UCS Manager Administration Management Guide* provides detailed information about configuring the device connector.

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 3: 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(8)	3.1(1)	3.1(2)	3.1(3)	3.2(1)	3.2(2)	3.2(3)
2.2(8)	6200	6200	6200	6200	6200	6200	6200
3.1(1)	—	6200,6332, 6332-16UP	6200,6332, 6332-16UP	6200,6332, 6332-16UP	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	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	6200,6332, 6332-16UP	6200,6332, 6332-16UP	6200,6332, 6332-16UP
3.2(1)	—	—	—	—	6200,6332, 6332-16UP	6200,6332, 6332-16UP	6200,6332, 6332-16UP
3.2(2)	—	—	—	—	6200,6332, 6332-16UP	6200,6332, 6332-16UP	6200,6332, 6332-16UP
3.2(3)	—	—	—	—	6200,6332, 6332-16UP	6200,6332, 6332-16UP	6200,6332, 6332-16UP

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

Table 4: Mixed Cisco UCS Releases Supported on Cisco UCS Mini Fabric Interconnects

	Infrastructure Versions (A Bundles)					
Host FW Versions (B or C Bundles)	3.1(1)	3.1(2)	3.1(3)	3.2(1)	3.2(2)	3.2(3)
3.1(1)	6324	6324	6324	6324	6324	6324
3.1(2)	6324	6324	6324	6324	6324	6324
3.1(3)	6324	6324	6324	6324	6324	6324
3.2(1)	—	—	—	6324	6324	6324
3.2(2)	—	—	—	6324	6324	6324
3.2(3)	—	—	—	6324	6324	6324

The following table lists the mixed B, C bundles that are supported on all platforms with the 3.2(1)A bundle:

Table 5: Mixed B, C Bundles Supported on All Platforms with the 3.2(1)A Bundle

	Infrastructure Versions (A Bundles)		
Host FW Versions (B, C Bundles)	3.2(1)		
	6200	6300	6324
	ucs-k9-bundle-infra.3.2.x.xxx.A.bin	ucs-6300-k9-bundle-infra.3.2.x.xxx.A.bin	ucs-mini-k9-bundle-infra.3.2.x.xxx.A.bin
2.2(8) (B, C Bundles)	Yes	—	—
3.1(1), 3.1(2), 3.1(3) (B, C Bundles)	Yes	Yes	Yes
3.2(1), 3.2(2), 3.2(3) (B, C Bundles)	Yes	Yes	Yes

The following table lists the mixed B, C bundles that are supported on all platforms with the 3.2(2)A bundle:

Table 6: Mixed B, C Bundles Supported on All Platforms with the 3.2(2)A Bundle

	Infrastructure Versions (A Bundles)		
Host FW Versions (B, C Bundles)	3.2(2)		
	6200	6300	6324
	ucs-k9-bundle-infra.3.2.x.xxx.A.bin	ucs-6300-k9-bundle-infra.3.2.x.xxx.A.bin	ucs-mini-k9-bundle-infra.3.2.x.xxx.A.bin
2.2(8) (B, C Bundles)	Yes	—	—
3.1(1), 3.1(2), 3.1(3) (B, C Bundles)	Yes	Yes	Yes
3.2(1), 3.2(2), 3.2(3) (B, C Bundles)	Yes	Yes	Yes

The following table lists the mixed B, C bundles that are supported on all platforms with the 3.2(3)A bundle:

Table 7: Mixed B, C Bundles Supported on All Platforms with the 3.2(3)A Bundle

	Infrastructure Versions (A Bundles)		
Host FW Versions (B, C Bundles)	3.2(3)		
	6200	6300	6324
	ucs-k9-bundle-infra.3.2.x.xxx.A.bin	ucs-6300-k9-bundle-infra.3.2.x.xxx.A.bin	ucs-mini-k9-bundle-infra.3.2.x.xxx.A.bin
2.2(8) (B, C Bundles)	Yes	—	—
3.1(1), 3.1(2), 3.1(3) (B, C Bundles)	Yes	Yes	Yes
3.2(1), 3.2(2), 3.2(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.

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 8: 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(8a) 2.2(8a)	3.1(1e) 3.1(1e)	3.1(1e)	3.2(3p)
B200 M2	2.2(8a)	3.1(1e)	3.1(1e)	3.2(3p)
B200 M3 E5-2600 B200 M3 E5-2600 v2	2.2(8a) 2.2(8a)	3.1(1e) 3.1(1e)	3.1(1e)	3.2(3p)
B200 M4	2.2(8a)	3.1(1e)	3.1(1e)	3.2(3p)
B200 M5	3.2(1d)	3.2(1d)	3.2(1d)	3.2(3p)
B230 M2	2.2(8a)	3.1(1e)	3.1(1e)	3.2(3p)
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(8a) 2.2(8a) 2.2(8a) 2.2(8a) 2.2(8a)	3.1(1e) 3.1(1e) 3.1(1e) 3.1(1e) 3.1(1e)	3.1(1e)	3.2(3p)
B260 M4 E7-4800 v4 B260 M4 E7-8800 v4	2.2(8b) 2.2(8b)	3.1(1e) 3.1(1e)	3.1(2b) 3.1(2b)	3.2(3p)

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
B420 M3 E5-4600 B420 M3 E5-4600 v2	2.2(8a) 2.2(8a)	3.1(1e) 3.1(1e)	3.1(1e)	3.2(3p)
B440 M2	2.2(8a)	3.1(1e)	3.1(1e)	3.2(3p)

B420 M4 E5-4600 v3
B420 M4 E5-4600 v4
	2.2(8a)
	2.2(8b)
		3.1(1e)
		3.1(1e)
			3.1(1e)
			3.1(2b)
				3.2(3p)
				3.2(3p)

B460 M4 E7-4800 v2 B460 M4 E7-8800 v2 B460 M4 E7-4800 v3 B460 M4 E7-8800 v3	2.2(8a) 2.2(8a) 2.2(8a) 2.2(8a)	3.1(1e) 3.1(1e) 3.1(1e) 3.1(1e)	3.1(1e)	3.2(3p)
B460 M4 E7-4800 v4 B460 M4 E7-8800 v4	2.2(8b) 2.2(8b)	3.1(1e) 3.1(1e)	3.1(2b)	3.2(3p)
B480 M5	3.2(2b)	3.2(2b)	3.2(2b)	3.2(3p)

Rack Servers

Table 9: Minimum Host Firmware Versions for Rack Servers

Servers	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Recommended Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI
C22 M3 and M3L	2.2(8a)	3.1(1e)	3.2(3p)
C24 M3, M3L, and M3S2	2.2(8a)	3.1(1e)	3.2(3p)
C220 M3	2.2(8a)	3.1(1e)	3.2(3p)
C220 M4	2.2(8a)	3.1(1e)	3.2(3p)
C220 M5	3.2(1d)	3.2(1d)	3.2(3p)

Servers	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Recommended Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI
C240 M3	2.2(8a)	3.1(1e)	3.2(3p)
C240 M4	2.2(8a)	3.1(1e)	3.2(3p)
C240 M5	3.2(1d)	3.2(1d)	3.2(3p)
C460 M4 E7-2800 v2	2.2(8a)	3.1(1e)	3.2(3p)
C460 M4 E7-4800 v2	2.2(8a)	3.1(1e)	
C460 M4 E7-8800 v2	2.2(8a)	3.1(1e)	
C460 M4 E7-4800 v3	2.2(8a)	3.1(1e)	
C460 M4 E7-8800 v3	2.2(8a)	3.1(1e)	
C460 M4 E7-8800 v4	2.2(8b)	3.1(1e)	3.2(3p)
C480 M5	3.2(2b)	3.2(2b)	3.2(3p)
S3260 M4	3.1(2b)	3.1(2b)	3.2(3p)
S3260 M5	3.2(3a)	3.2(3a)	3.2(3p)

Adapters

Table 10: 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-BD16GF	3.2(3a)	3.2(3a)	3.2(3a)	3.2(3p)
UCSC-PCIE-ID40GF	3.2(3a)	3.2(3a)	3.2(3a)	3.2(3p)
UCSC-PCIE-IQ10GF	3.2(3a)	3.2(3a)	3.2(3a)	3.2(3p)
UCSC-PCIE-ID10GF	3.2(3a)	3.2(3a)	3.2(3a)	3.2(3p)

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
XXV710-DA2	3.2(3a)	3.2(3a)	3.2(3a)	3.2(3p)
UCSC-PCIE-ID10GC	3.2(3a)	3.2(3a)	3.2(3a)	3.2(3p)
N2XX-AIPCI01	3.2(3a)	3.2(3a)	3.2(3a)	3.2(3p)
UCSC-PCIE-ID25GF	3.2(3a)	3.2(3a)	3.2(3a)	3.2(3p)
UCSC-PCIE-QD25GF	3.2(2b)	3.2(2b)	3.2(2b)	3.2(3p)
UCSC-PCIE-QD40GF	3.2(2b)	3.2(2b)	3.2(2b)	3.2(3p)
UCSC-PCIE-IQ10GC	3.2(2b)	3.2(2b)	3.2(2b)	3.2(3p)
UCSC-PCIE-QD16GF	3.2(1d)	3.2(1d)	3.2(1d)	3.2(3p)
UCSC-PCIE-C40Q-03 UCSC-MLOM-C40Q-03	2.2(8a)	3.1(1e)	3.1(1e)	3.2(3p)
UCS-VIC-M82-8P UCSB-MLOM-40G-01 UCSB-MLOM-PT-01	2.2(8a)	3.1(1e)	3.1(1e)	3.2(3p)
UCSB-MLOM-40G-03 UCSB-VIC-M83-8P UCSC-MLOM-CSC-02	2.2(8a)	3.1(1e)	3.1(1e)	3.2(3p)
UCSC-PCIE-CSC-02	2.2(8a)	3.1(1e)	3.1(1e)	3.2(3p)
UCSC-F-FIO-1000MP UCSC-F-FIO-1300MP UCSC-F-FIO-2600MP UCSC-F-FIO-5200MP	2.2(8a)	3.1(1e)	3.1(1e)	3.2(3p)
UCSB-FIO-1600MS UCSB-FIO-1300MS	2.2(8a)	3.1(1e)	3.1(1e)	3.2(3p)

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-INVADER-3108 UCSC-NYTRO-200GB	2.2(8a)	3.1(1e)	3.1(1e)	3.2(3p)
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(8a)	3.1(1e)	3.1(1e)	3.2(3p)
UCS-PCIE-E14102B	2.2(8a)	3.1(1g)	3.1(1g)	3.2(3p)
UCSC-PCIE-IQ10GF UCSC-PCIE-ID10GF UCSC-PCIE-ID40GF	—	—	3.1(2b)	3.2(3p)

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-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-PCI25-38001	—	3.1(2b)	3.1(2b)	3.2(3p)
UCSC-PCIE-QD32GF N2XX-AQPCI05 UCSC-PCIE-Q2672 UCSC-PCIE-BD32GF UCSC-PCIE-BS32GF N2XX-AEPCI05	—	3.1(3a)	3.1(3a)	3.2(3p)
UCSC-PCIE-E16002	—	3.2(1d)	3.2(1d)	3.2(3p)
UCSC-PCIE-ID10GC	3.1(2b)	3.1(2b)	3.1(2b)	3.1(2b)

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

Type	Details
Chassis	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 12: Supported Hardware for UCS 6200 Fabric Interconnects

Type	Details
Chassis	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, transceiver modules, and supported cables:

Table 13: Supported Cables for GB Connector Modules

GB Connector Modules	Transceiver Modules and 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
16-GB	DS-SFP-FC16G-LW DS-SFP-FC16G-SW

GB Connector Modules	Transceiver Modules and Cables
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 [1]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

[1] 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)	3.2(3p)
UCSB-5108-DC2	3.0(2c)	3.2(3p)

UCS Mini Supported Blade and Rack Servers

Servers	Minimum Software Version	Recommended Software Version
B200 M5	3.2(1d)	3.2(3p)
B200 M3	3.1(1e)	3.2(3p)
B200 M4	3.1(1e)	3.2(3p)
B260 M4	3.1(2b)	3.2(3p)
B420 M3	3.1(1e)	3.2(3p)
B420 M4	3.1(1e)	3.2(3p)
B460 M4	3.1(2b)	3.2(3p)
B480 M5	3.2(2b)	3.2(3p)
B22 M3	3.1(1e)	3.2(3p)
C220 M3	3.1(1e)	3.2(3p)
C240 M3	3.1(1e)	3.2(3p)
C220 M4	3.1(1e)	3.2(3p)
C240 M4	3.1(1e)	3.2(3p)
C220 M5	3.2(1d)	3.2(3p)
C240 M5	3.2(1d)	3.2(3p)
C480 M5	3.2(2b)	3.2(3p)

UCS Mini Supported Adapters

Adapters	Minimum Software Version	Recommended Software Version
UCSC-PCIE-IQ10GC UCSC-PCIE-QD25GF UCSC-PCIE-QD40GF	3.2(2b)	3.2(3p)
UCSC-PCIE-C40Q-03 UCSC-MLOM-C40Q-03	3.1(1e)	3.2(3p)
UCS-VIC-M82-8P UCSB-MLOM-40G-01 UCSB-MLOM-PT-01	3.1(1e)	3.2(3p)

Adapters	Minimum Software Version	Recommended Software Version
UCSB-MLOM-40G-03 UCSB-VIC-M83P-8P UCSC-MLOM-CSC-02	3.1(1e)	3.2(3p)
UCSC-PCIE-CSC-02	3.1(1e)	3.2(3p)

UCS Mini Supported Fabric Interconnects

Fabric Interconnects	Minimum Software Version	Recommended Software Version
Cisco UCS 6324	3.1(1e)	3.2(3p)

UCS Mini Supported Fabric Extenders for Secondary Chassis

Fabric Extenders	Minimum Software Version	Recommended Software Version
UCS 2204 XP	3.1(1e)	3.2(3p)
UCS 2208 XP	3.1(1e)	3.2(3p)

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	3.1(1e)	3.2(3p)

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
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

Gb Connector Modules	Cables
1-GB	GLC-GE-T GLC-LH-SM GLC-SX-MM GLC-T (V03 or higher)

Upgrade and Downgrade Guidelines

See the *Cisco UCS Manager Firmware Management Guide*, Release 3.2 section Firmware Upgrade to Cisco UCS Manager Release 3.2 for detailed upgrade paths.

The following are a few reminders before you plan to upgrade to or downgrade from Cisco UCS Manager, Release 3.2(3):

- If single path access is enabled, you cannot downgrade to any release earlier than 3.2(3a).
- If **6G-12G Mixed Mode** is enabled, you cannot downgrade to any release earlier than 3.2(3a).

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.

Starting with Cisco UCS Manager Release 3.2(3a), the deprecated third-party adapters (vNIC & vHBA) support is limited to inventory and firmware management in Cisco UCS Manager. For more information, see Deprecated Hardware and Software in Cisco UCS Manager Release 3.2, on page 14

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 14: Version Mapping

UCS Release	Catalog File Name	Additional PIDs In This Release
3.2(3p)	ucs-catalog.3.2.3l.T.bin	Drive: • UCS-HD12T7KL4NK9 Drives for UCS S3260 M5: • UCS-S-HD12TK9 • UCS-S-HD12TRK9
3.2(3o)	ucs-catalog.3.2.3k.T.bin	—
3.2(3n)	ucs-catalog.3.2.3k.T.bin	—

UCS Release	Catalog File Name	Additional PIDs In This Release
3.2(3l)	ucs-catalog.3.2.3j.T.bin	—
3.2(3k)	ucs-catalog.3.2.3j.T.bin	—
3.2(3j)	ucs-catalog.3.2.3i.T.bin	—
3.2(3i)	ucs-catalog.3.2.3i.T.bin	Drives: • UCS-SD480GBHBNK9 • UCS-SD960GBHBNK9 • UCS-SD38TBHBNK9 • UCS-SD480GBHTNK9 • UCS-SD960GBHTNK9 • UCS-SD38TBHTNK9
3.2(3h)	ucs-catalog.3.2.3h.T.bin	—
3.2(3g)	ucs-catalog.3.2.3f.T.bin	Drives: • UCS-SD480GM3X-EP • UCS-SD960GM3X-EP • UCS-SD19TM3X-EP
3.2(3e)	ucs-catalog.3.2.3e.T.bin	—
3.2(3d)	ucs-catalog.3.2.3d.T.bin	Drives: • UCS-HD24T10NK9
3.2(3b)	ucs-catalog.3.2.3b.T.bin	Drives: • UCS-SD480GH1-EV • UCS-SD960GH1-EV • UCS-SD19TH1-EV • UCS-SD38TH1-EV • UCS-SD400GBHK9 • UCS-SD800GBHK9 • UCS-SD16TBHK9 • UCS-S3260-TSD4K9

UCS Release	Catalog File Name	Additional PIDs In This Release
3.2(3a)	ucs-catalog.3.2.3a.T.bin	

UCS Release	Catalog File Name	Additional PIDs In This Release
		Cisco UCS S-Series Rack Server: • UCS-S3260-M5SRB Cisco UCS S3260 M5 CPUs: • UCS-CPU-4110 • UCS-CPU-4114 • UCS-CPU-5118 • UCS-CPU-6132 • UCS-CPU-6138 • UCS-CPU-6152 Memory for UCS S3260 M5: • UCS-MR-X16G1RS-H • UCS-MR-X32G2RS-H • UCS-ML-X64G4RS-H NVME SSDs for UCS S3260 M5: • UCS-S3260-NVM48 • UCS-S3260-NVM416 • UCS-S3260-NVM438 • UCS-S3260-NVM464 • UCS-S3260-NVG25 • UCS-S3260-NVG210 • UCS-S3260-NVG220 Storage Controller for UCS S3260 M5: • UCS-S3260-DHBA • UCS-S3260-DRAID Disk Expansion Tray for UCS S3260 M5: • UCS-S3260-SFFET Drives for UCS S3260 M5: • UCS-HD18TB10KS4K • UCS-HD12TB10K12G • UCS-SD16TB12S4-EP

UCS Release	Catalog File Name	Additional PIDs In This Release
		• UCS-SD800GSAS3-EP Cisco UCS B200 M5 CPUs: • UCS-CPU-5117 • UCS-CPU-8180 • UCS-CPU-8168 • UCS-CPU-6154 • UCS-CPU-8180M Cisco UCS NVMe-Optimized Rack-Mount Servers: • UCSC-C220-M5SN • UCSC-C240-M5SN • UCS-C480-M5 NVME SSDs for NVMe-optimized UCS M5 servers: • UCSC-NVMEXP-I375 • UCSB-NVMEHW-I1600 • UCSB-NVMEHW-I2000 • UCSB-NVMEHW-I3200 • UCSB-NVMEHW-I1000 • UCSB-NVMEHW-I2TBV • UCSB-NVMEHW-I4000 • UCSB-NVMELW-I500 • UCSB-NVMELW-I1000 • UCSB-NVMELW-I2000
3.2(2f)	ucs-catalog.3.2.2i.T.bin	—
3.2(2d)	ucs-catalog.3.2.2e.T.bin	—

UCS Release	Catalog File Name	Additional PIDs In This Release
3.2(2c)	ucs-catalog.3.2.2e.T.bin	Drives: • UCS-HD12T7KL4KHM • UCS-S3260-HD12T • UCS-S3260-HD12TR • UCS-HD12T7KL4KN • UCS-HD12T7KL6GN

UCS Release	Catalog File Name	Additional PIDs In This Release
3.2(2b)	ucs-catalog.3.2.2b.T.bin	

UCS Release	Catalog File Name	Additional PIDs In This Release
		Cisco UCS Blade Server: • UCSB-B480-M5 Cisco UCS B480 M5 CPUs: • UCS-CPU-8180 • UCS-CPU-8176 • UCS-CPU-8170 • UCS-CPU-8164 • UCS-CPU-8160 • UCS-CPU-8153 • UCS-CPU-6152 • UCS-CPU-6148 • UCS-CPU-6138 • UCS-CPU-6140 • UCS-CPU-6130 • UCS-CPU-5120 • UCS-CPU-5118 • UCS-CPU-8168 • UCS-CPU-8158 • UCS-CPU-8156 • UCS-CPU-6154 • UCS-CPU-6150 • UCS-CPU-6142 • UCS-CPU-6132 • UCS-CPU-6144 • UCS-CPU-6136 • UCS-CPU-6126 • UCS-CPU-6146 • UCS-CPU-6134 • UCS-CPU-6128 • UCS-CPU-5122 • UCS-CPU-5115

UCS Release	Catalog File Name	Additional PIDs In This Release
		- UCS-CPU-8180M - UCS-CPU-6142M - UCS-CPU-6134M - UCS-CPU-8176M - UCS-CPU-8170M - UCS-CPU-8160M - UCS-CPU-6140M Cisco UCS Rack-Mount Server: - UCSC-C480-M5 Cisco UCS C480 M5 CPUs:

UCS Release	Catalog File Name	Additional PIDs In This Release
		• UCS-CPU-8180 • UCS-CPU-8176 • UCS-CPU-8170 • UCS-CPU-8164 • UCS-CPU-8160 • UCS-CPU-8153 • UCS-CPU-6152 • UCS-CPU-6148 • UCS-CPU-6138 • UCS-CPU-6130 • UCS-CPU-5120 • UCS-CPU-8168 • UCS-CPU-8158 • UCS-CPU-8156 • UCS-CPU-6154 • UCS-CPU-6150 • UCS-CPU-6142 • UCS-CPU-6136 • UCS-CPU-6126 • UCS-CPU-6134 • UCS-CPU-8180M • UCS-CPU-6142M • UCS-CPU-8176M • UCS-CPU-8170M • UCS-CPU-8160M • UCS-CPU-6140M Memory for UCS B480 M5 and C480 M5:

UCS Release	Catalog File Name	Additional PIDs In This Release
		• UCS-MR-X16G1RS-H • UCS-MR-X32G2RS-H • UCS-MR-X64G4RS-H • UCS-ML-X64G4RS-H • UCS-MR-128G8RS-H • UCS-ML-X32G2RS-H (B480 M5 only) • UCS-MR-X16G2RS-H (C480 M5 only) Qlogic adapters: • UCSC-PCIE-QD25GF • UCSC-PCIE-QD40GF Intel adapter: • UCSC-PCIE-IQ10GC NVIDIA P4 GPUs with the C240 M5 rack-mount server: • UCSC-GPU-P4 NVME Devices: • UCSC-NVMEHW-H800 • UCSC-NVMEM4-H800 • UCSC-NVMEHW-H1600 • UCSC-NVMEM4-H1600 • UCSC-NVME-H64003 • UCSC-NVME-H76801

UCS Release	Catalog File Name	Additional PIDs In This Release
3.2(1d)	ucs-catalog.3.2.1d.T.bin	

UCS Release	Catalog File Name	Additional PIDs In This Release
		Cisco UCS Blade Server: • UCSB-B200-M5 Cisco UCS B200 M5 CPUs: • UCS-CPU-8176 • UCS-CPU-8164 • UCS-CPU-8160 • UCS-CPU-6152 • UCS-CPU-6148 • UCS-CPU-6142 • UCS-CPU-6140 • UCS-CPU-6138 • UCS-CPU-6134 • UCS-CPU-6132 • UCS-CPU-6130 • UCS-CPU-6128 • UCS-CPU-5122 • UCS-CPU-5120 • UCS-CPU-5118 • UCS-CPU-5115 • UCS-CPU-4116 • UCS-CPU-4114 • UCS-CPU-4112 • UCS-CPU-4110 • UCS-CPU-4108 • UCS-CPU-3106 • UCS-CPU-3104 • UCS-CPU-8176M • UCS-CPU-6142M • UCS-CPU-6134M Cisco UCS Rack-Mount Servers:

UCS Release	Catalog File Name	Additional PIDs In This Release
		- UCSC-C220-M5 - UCSC-C240-M5 Cisco UCS C220 M5 and C240 M5 CPUs:

UCS Release	Catalog File Name	Additional PIDs In This Release
		• UCS-CPU-8180M • UCS-CPU-6142M • UCS-CPU-6134M • UCS-CPU-8176M • UCS-CPU-8170M • UCS-CPU-8160M • UCS-CPU-6140M • UCS-CPU-8180 • UCS-CPU-8176 • UCS-CPU-8170 • UCS-CPU-8168 • UCS-CPU-8164 • UCS-CPU-8160 • UCS-CPU-8158 • UCS-CPU-8156 • UCS-CPU-8153 • UCS-CPU-6154 • UCS-CPU-6152 • UCS-CPU-6150 • UCS-CPU-6148 • UCS-CPU-6142 • UCS-CPU-6140 • UCS-CPU-6138 • UCS-CPU-6136 • UCS-CPU-6134 • UCS-CPU-6132 • UCS-CPU-6130 • UCS-CPU-6128 • UCS-CPU-6126 • UCS-CPU-5122 • UCS-CPU-5120

UCS Release	Catalog File Name	Additional PIDs In This Release
		• UCS-CPU-5118 • UCS-CPU-5115 • UCS-CPU-4116 • UCS-CPU-4114 • UCS-CPU-4112 • UCS-CPU-4110 • UCS-CPU-4108 • UCS-CPU-3106 • UCS-CPU-3104 • UCS-CPU-5120T • UCS-CPU-8160T • UCS-CPU-6130T • UCS-CPU-6130F Memory for UCS B200 M5, C220 M5 and C240 M5: • UCS-MR-X16G1RS-H • UCS-MR-X32G2RS-H • UCS-MR-X64G4RS-H • UCS-ML-X64G4RS-H • UCS-MR-128G8RS-H • UCS-MR-X16G2RS-H (C220 M5 and C240 M5 only) • UCS-MR-X8G1RS-H (C220 M5 and C240 M5 only) Qlogic adapter: • UCSC-PCIE-QD16GF NVIDIA P6 GPUs with the B200 M5 blade server: • UCSB-GPU-P6-F • UCSB-GPU-P6-R NVIDIA P40 GPUs with the C220 M5 and C240 M5 rack-mount servers:

UCS Release	Catalog File Name	Additional PIDs In This Release
		• UCSC-GPU-P40 Storage Modules: • SD—UCS-MSTOR-SD • SATA—UCS-MSTOR-M2 SD Cards: • UCS-SD-32G-S • UCS-SD-64G-S • UCS-SD-128G M.2 SATA Drives: • UCS-M2-240GB • UCS-M2-960GB NVME Devices: • UCSC-NVMEHW-H800 • UCSC-NVMEHW-H1600 • UCSC-NVMEHW-H3200 • UCSC-NVMEHW-H6400 • UCSC-NVMEHW-H7680 • UCSC-NVMEHY-H800 • UCSC-NVMEHY-H1600 • UCSC-NVMEHY-H3200 • UCSC-NVME-H16003 • UCSC-NVME-H32003 • UCSC-NVME-H38401 • UCSC-NVME-H64003 • UCSC-NVME-H76801

Security Fixes

The following security issues are resolved:

Release	Defect ID	CVE	Description
3.2(3p)	CSCvt86093	- CVE-2020-0548 - CVE-2020-0549	Cisco UCS M5 servers that are based on Intel® processors are affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID(s): - CVE-2020-0548: Clean-up errors in some Intel® Processors may allow an authenticated user to potentially enable information disclosure via local access. - CVE-2020-0549: Clean-up errors in some data cache evictions for some Intel® Processors may allow an authenticated user to potentially enable information disclosure via local access. This release includes BIOS revisions for Cisco UCS M5 servers. These BIOS revisions include Microcode update for Cisco UCS M5 servers, which is a required part of the mitigation for these vulnerabilities.
3.2(3p)	CSCvp62709	CVE-2019-11358	Cisco UCS Manager and UCS 6400 Series Fabric Interconnects using the jQuery software package with versions from 1.2 to 3.5.0, is affected by the following Common Vulnerability and Exposures (CVE) ID: - CVE-2019-11358: In jQuery versions greater than or equal to 1.2 and before 3.5.0, as used in Drupal, Backdrop CMS, and other products, jQuery.extend(true, {}, ...) is mishandled because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype. This problem is patched in jQuery 3.5.0 . The jQuery library has been upgraded to the latest version, which contains the fix.
3.2(3p)	CSCvu53094	CVE-2020-11022	Cisco UCS Manager and UCS 6400 Series Fabric Interconnects using the jQuery software package with versions from 1.2 to 3.5.0, is affected by the following Common Vulnerability and Exposures (CVE) ID: - CVE-2020-11022: In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. The jQuery library has been upgraded to the latest version, which contains the fix.

Release	Defect ID	CVE	Description
3.2(3o)	CSCvp62709 CSCvp69717	CVE-2019-11358	Cisco UCS Manager and UCS 6200 Series Fabric Interconnects included a version of the jQuery software package that is affected by the cross-site scripting vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs: CVE-2019-11358: jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype. Additional information on Cisco's security vulnerability policy can be found here: Security Vulnerability Policy
3.2(3o)	CSCvs81686	• CVE-2020-0548 • CVE-2020-0549	Cisco UCS M5 servers that are based on Intel® processors are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs: • CVE-2020-0548 Cleanup errors in some Intel® Processors may allow an authenticated user to potentially enable information disclosure via local access. • CVE-2020-0549 Cleanup errors in some data cache evictions for some Intel® Processors may allow an authenticated user to potentially enable information disclosure via local access. This release includes BIOS revisions for Cisco UCS M5 servers. These BIOS revisions include the updated SINIT ACM for Cisco UCS M5 servers, which is a required part of the mitigation for these vulnerabilities.

Release	Defect ID	CVE	Description
3.2(3o)	CSCvr54409 CSCvr54415	• CVE-2019-11135 • CVE-2019-0151 • CVE-2019-0152 • CVE-2019-11136 • CVE-2019-11137 • CVE-2019-11139 • CVE-2019-11109	

Release	Defect ID	CVE	Description
			Cisco UCS M5 servers that are based on Intel® processors are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs: • CVE-2019-11135 (TSX Asynchronous Abort Advisory) condition affects certain 2nd Generation Intel® Xeon® Scalable Processors, 8th Generation Intel® Core™ Processor Family, 9th Generation Intel® CoreTM Processor Family, and 10th Generation Intel® Core™ Processor Family that utilize speculative execution, and may allow an authenticated user to potentially enable information disclosure through a side-channel with local access. • 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-2019-0152 (CPU Local Privilege Escalation Advisory) affects certain Intel® Xeon® Scalable Processors, Intel® Xeon® Processor D-2100, D-3100, Intel® Xeon® Processor W-2100, W-3100 when insufficient memory protection may allow a privileged user to potentially enable an escalation of privilege through local access. This could result in bypassing System Management Mode (SMM) and Intel® TXT protections. • CVE-2019-11136 (BIOS 2019.2 IPU Advisory) affects 2nd Generation Intel® Xeon® Scalable Processors, Intel® Xeon® Scalable Processors, Intel® Xeon® Processor D Family when insufficient access control 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. • CVE-2019-11137 (BIOS 2019.2 IPU Advisory) affects

Release	Defect ID	CVE	Description
			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. • CVE-2019-11139 (Voltage Modulation Technical Advisory) vulnerability in voltage modulation of certain Intel® Xeon® Scalable Processors may allow a privileged user to potentially enable denial of service through local access. • CVE-2019-11109: Logic issue in subsystem in Intel® Server Platform Services before versions SPS_E5_04.01.04.297.0, SPS_SoC-X_04.00.04.101.0, and SPS_SoC-A_04.00.04.193.0 may allow a privileged user to potentially enable Denial of Service through local. This release includes BIOS revisions for Cisco UCS M5 servers. These BIOS revisions include the updated microcode and Secure Initialization (SINIT) Authenticated Code Modules (ACM), which are required parts of the mitigation for these vulnerabilities.

Release	Defect ID	CVE	Description
3.2(3n)	CSCvq19565	CVE-2019-11479 CVE-2019-11478	UCS 6200 Series Fabric Interconnects are affected by the vulnerability identified by the following CVE IDs: • CVE-2019-11479: Excess Resource Consumption Due to Low MSS Values • CVE-2019-11478: SACK Slowness or Excess Resource Usage TCP networking vulnerabilities have been identified affecting Linux kernel. The vulnerabilities specifically relate to the minimum segment size (MSS) and TCP Selective Acknowledgement (SACK) capabilities. The most serious, dubbed "SACK Panic" allows a remotely-triggered kernel panic on recent Linux kernels. Cisco UCS 6200 Series Fabric Interconnects have been determined to contain a vulnerable version of Linux Kernel. However the product is not affected by the following vulnerability: CVE-2019-11477: SACK Kernel Panic Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability. Additional details about the vulnerabilities listed above can be found at http://cve.mitre.org/cve/cve.html

Release	Defect ID	CVE	Description
3.2(3n)	CSCvr15082	CVE-2020-3120	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. **Note** Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). 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: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-fxnxos-iosxr-cdp-dos
3.2(3n)	CSCvr37150	—	A vulnerability in the Cisco Discovery Protocol feature of Cisco FXOS Software and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code as root or cause a denial of service (DoS) condition on an affected device. The vulnerability exists because of insufficiently validated Cisco Discovery Protocol packet headers. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to a Layer 2-adjacent affected device. A successful exploit could allow the attacker to cause a buffer overflow that could allow the attacker to execute arbitrary code as root or cause a DoS condition on the affected device. Note: Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

Release	Defect ID	CVE	Description
3.2(3n)	CSCvq33385	CVE-2016-2183	The latest CiscoSSL 1.0.2r.6.2.341 now automatically fixes the OpenSSL vulnerabilities in Cisco UCS Manager identified by the Common Vulnerability and Exposures (CVE) ID listed.
3.2(3n)	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$^{\text{TM}}$ Processors, 5th Generation Intel® Core$^{\text{TM}}$ Processors, 6th Generation Intel® Cores Processors, 7th Generation Intel® Core$^{\text{TM}}$ Processors, 8th Generation Intel® Core$^{\text{TM}}$ 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
3.2(3n)	CSCvr54413 CSCvr54414	CVE-2019-0151 CVE-2019-11137	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 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.

Release	Defect ID	CVE	Description
3.2(3l)	CSCvo21412 CSCvp30013	CVE-2018-12126 CVE-2018-12127 CVE-2018-12130 CVE-2019-11091	Cisco UCS M4 servers and Hyperflex M4 servers are based on Intel® Xeon® Processor E7 v2, v3, and v4 Product Family processors that 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 Cisco UCS M4 generation servers. These BIOS revisions include the updated microcode that is a required part of the mitigation for these vulnerabilities.

Release	Defect ID	CVE	Description
3.2(31)	CSCvp28016	CVE-2018-12126 CVE-2018-12127 CVE-2018-12130 CVE-2019-11091	Cisco UCS M4 servers and Hyperflex M4 servers are based on Intel® Xeon® Processor E5 v3 and v4 Product Family processors that 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 Cisco UCS M4 generation servers. These BIOS revisions include the updated microcode that is a required part of the mitigation for these vulnerabilities. Additional details about the vulnerabilities listed above can be found at http://cve.mitre.org/cve/cve.html

Release	Defect ID	CVE	Description
3.2(31)	CSCvp31847	CVE-2018-12126 CVE-2018-12127 CVE-2018-12130 CVE-2019-11091	Cisco UCS M5 servers and Hyperflex M5 servers are based on Intel® Xeon® Scalable processors that 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 Cisco UCS M5 generation servers. These BIOS revisions include the updated microcode that is a required part of the mitigation for these vulnerabilities.

Release	Defect ID	CVE	Description
3.2(3l)	CSCvp27917	CVE-2018-12126 CVE-2018-12127 CVE-2018-12130 CVE-2019-11091	Cisco UCS B-Series M3 Blade Servers are based on Intel® Xeon® Sandy Bridge E5-2600 and Ivy Bridge E5 2600 v2 Product Family processors that 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 Cisco UCS M3 generation servers. These BIOS revisions include the updated microcode that is a required part of the mitigation for these vulnerabilities. Additional details about the vulnerabilities listed above can be found at http://cve.mitre.org/cve/cve.html

Release	Defect ID	CVE	Description
3.2(31)	CSCvk70633	CVE-2019-1962	A vulnerability in the Cisco Fabric Services (CFS) component of Cisco NX-OS Software could have allowed an unauthenticated, remote attacker to cause process crashes that could have resulted in a denial of service (DoS) condition on an affected system. The vulnerability was due to insufficient validation of TCP packets when processed by the Cisco Fabric Services over IP (CFSoIP) feature. An attacker could exploit this vulnerability by sending a crafted CFS TCP packet to an affected device. A successful exploit could cause process crashes, resulting in a device reload and a DoS condition. **Note** Three distribution methods can be configured for CFS. This vulnerability only affects distribution method CFSoIP, which is disabled by default. See the Security Advisory for more information. 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: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/
3.2(31)	CSCvn23535	CVE-2019-1963	A vulnerability in the Simple Network Management Protocol (SNMP) input packet processor of Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, remote attacker to cause the SNMP application on an affected device to restart unexpectedly. The vulnerability was due to improper validation of Abstract Syntax Notation One (ASN.1) encoded variables in SNMP packets. An attacker could have exploited this vulnerability by sending a crafted SNMP packet to the SNMP daemon on the 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: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190828-fxnxos-snmp-dos

Release	Defect ID	CVE	Description
3.2(3l)	CSCvm80093	CVE-2019-1966	A vulnerability in the CLI implementation of a specific command for the Cisco UCS Fabric Interconnect could have allowed an authenticated, local attacker to escape the CLI and gain unauthorized access to the underlying operating system of the device. The vulnerability existed due to insufficient sanitization of user-supplied input that was passed to a specific CLI command of the affected device. An attacker could have exploited this vulnerability to escape the CLI and execute arbitrary commands on the underlying operating system with the privileges of the root user. The attacker would need valid device credentials. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html.
3.2(3l)	CSCvn11851 CSCvk52975	CVE-2019-1726 CVE-2019-1735	A vulnerability in the CLI of Cisco NX-OS Software could have allowed an authenticated, local attacker to access restricted internal services on an affected device, such as the NX-API. The vulnerability was due to insufficient validation of arguments passed to a specific CLI command. An attacker could have exploited this vulnerability by including malicious input as the argument to the affected command. A successful exploit could have allowed the attacker to bypass intended restrictions and access internal services of the device. An attacker would need valid device credentials to exploit this vulnerability. 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: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190515-nxos-cli-bypass

Release	Defect ID	CVE	Description
3.2(3k)	CSCvm86205	—	A vulnerability in the local management CLI implementation for specific commands on the Cisco UCS B-Series Blade Servers could have allowed an authenticated, local attacker to overwrite an arbitrary file on disk. It is also possible the attacker could inject CLI command parameters which should not be allowed for a specific subset of local management CLI commands. The vulnerability is due to lack of proper input validation of user input for local management CLI commands. An attacker could exploit this vulnerability by authenticating to the device and issuing a crafted form of a limited subset of local management CLI commands. An exploit could allow the attacker to overwrite an arbitrary files on disk or inject CLI command parameters which should have been disabled. 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: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-ucs-cli-inj
3.2(3k)	CSCvo60001	—	During a Nessus vulnerability scan of the UCS Fabric Interconnects, a weak MAC was detected on systems running Cisco UCS Manager. Cisco UCS 6200 Series Fabric Interconnects have adopted new secure code best practices to enhance the security posture and resiliency of the product.
3.2(3k)	CSCvm64944	—	During a Nessus vulnerability scan of the UCS Fabric Interconnects, weak KEX algorithms were detected running in Cisco UCS Manager. Cisco UCS 6200 Series Fabric Interconnects have adopted new secure code best practices to enhance the security posture and resiliency of the product.
3.2(3j)	CSCvn61411	—	A vulnerability in the diagnostic CLI command of the Cisco UCS 6200 Series and 6300 Series Fabric Interconnects may allow an authenticated local attacker to view sensitive information in the command output. The vulnerability is due to lack of proper masking of sensitive information before being written to the diagnostic support output. An attacker may exploit this vulnerability by authenticating to the targeted device and issuing a specific diagnostic CLI command. However, an attacker needs a valid user credentials to exploit this vulnerability. 3.2(3j) release includes the fix for this issue. Password hashes that show in the CLI command are now hidden.

Release	Defect ID	CVE	Description
3.2(3i)	CSCvk20775	CVE-2018-3655	Cisco UCS B-Series servers include a version of the Intel® Converged Security Management Engine (CSME) that maybe affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID: • CVE-2018-3655 An attacker with physical access could use these vulnerabilities to do the following: • Bypass Intel® CSME anti-replay protection, thus allowing potential brute force attacks on secrets stored inside the Intel CSME • Gain unauthorized access to the Intel® MEBX password • Tamper with the integrity of the Intel® CSME file system directories or the Server Platform Services and Trusted Execution Environment (Intel® TXE) data files This release includes BIOS revisions for Cisco UCS M5 generation B-Series servers.
3.2(3h)	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® EX 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

Release	Defect ID	CVE	Description
3.2(3g)	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
3.2(3g)	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
3.2(3g)	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
3.2(3g)	CSCvm03339	CVE-2018-3615 CVE-2018-3620 CVE-2018-3646	Cisco UCS B-Series M5 servers, C-Series M5 servers, and HyperFlex M5 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 M5 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

3.2(3g)
3.2(3a)
	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 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 now been addressed on all Fabric Interconnect platforms.
			For more information, refer to the Cisco Security Advisory available at the following links:
			Cisco FXOS and NX-OS System Software Authentication, Authorization, and Accounting Denial of Service Vulnerability

Release	Defect ID	CVE	Description
3.2(3g)	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, please see the Cisco Security Advisory available here: CPU Side-Channel Information Disclosure Vulnerabilities: May 2018
3.2(3g)	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, please see the Cisco Security Advisory available here: CPU Side-Channel Information Disclosure Vulnerabilities: May 2018

Release	Defect ID	CVE	Description
3.2(3g)	CSCvj59266	CVE-2018-3639 CVE-2018-3640	Cisco UCS M5 servers and Hyperflex M5 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 M5 and Hyperflex M5 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, please see the Cisco Security Advisory available here: CPU Side-Channel Information Disclosure Vulnerabilities: May 2018
3.2(3e)	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, please see the Cisco Security Advisory available here: CPU Side-Channel Information Disclosure Vulnerabilities: May 2018

Release	Defect ID	CVE	Description
3.2(3b)	CSCvh31576	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 Ex 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 available here: CPU Side-Channel Information Disclosure Vulnerabilities
3.2(3a)	CSCve59744	CVE-2017-15361	The vulnerability related to TPM 2.0 is addressed.
3.2(3a)	CSCvf23655 (for software patch) CSCvf31495 (for software image)	CVE-2017-12331 (for software patch) CVE-2017-12333 (for software image)	A vulnerability in Cisco NX-OS System Software could allow an authenticated, local attacker to bypass signature verification when loading a software patch or image. This vulnerability has been fixed. For more information, refer to the Cisco Security Advisory available at the following links: • Cisco NX-OS System Software Patch Signature Bypass Vulnerability • Cisco NX-OS System Software Image Signature Bypass Vulnerability

Release	Defect ID	CVE	Description

3.2(3a)
3.2(2f)
	CSCvg97982
	CSCvh31577
	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 BIOS revisions for Cisco UCS M3, M4, M5, and Hyperflex M4, and M5 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 available here:
			CPU Side-Channel Information Disclosure Vulnerabilities

3.2(2e)	CSCvg97982 CSCvh31577	CVE-2017-5753 CVE-2017-5715 CVE-2017-5754	This is a software advisory for the Side Channel Analysis vulnerability that impacts UCS M5 servers. For more information, see the following software advisory: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/SA/SW_Advisory_CSCvh31577_CSCvg97982.html

Release	Defect ID	CVE	Description
3.2(2b)	CSCvd72179	CVE-2017-6464 CVE-2017-6462 CVE-2017-6463 CVE-2017-6458 CVE-2017-6451 CVE-2017-6460 CVE-2016-9042 CVE-2017-6455 CVE-2017-6452 CVE-2017-6459 CVE-2015-8138 CVE-2016-7431	Cisco UCS Manager included a version of NTPd that was affected by the vulnerability identified by one or more of the following Common Vulnerability and Exposures (CVE) IDs. These CVE IDs no longer impact any Cisco UCS Manager release: • CVE-2017-6464—NTP-01-016 NTP: Denial of Service via Malformed Config • CVE-2017-6462—NTP-01-014 NTP: Buffer Overflow in DPTS Clock • CVE-2017-6463—NTP-01-012 NTP: Authenticated DoS via Malicious Config Option • CVE-2017-6458—NTP-01-004 NTP: Potential Overflows in ctl_put() functions • CVE-2017-6451—NTP-01-003 Improper use of snprintf() in mx4200_send() • CVE-2017-6460—NTP-01-002 Buffer Overflow in ntpq when fetching reslist • CVE-2016-9042—Network Time Protocol Origin Timestamp Check Denial of Service Vulnerability Cisco UCS Manager is not affected by the following CVE IDs: • CVE-2017-6455—NTP-01-009 NTP: Windows: Privileged execution of User Library code • CVE-2017-6452—NTP-01-008 NTP: Windows Installer: Stack Buffer Overflow from Command Line • CVE-2017-6459—NTP-01-007 NTP: Windows Installer: Data Structure terminated insufficiently • CVE-2015-8138—Zero Origin Timestamp Bypass • CVE-2016-7431—Zero Origin Timestamp Bypass
3.2(2b)	CSCvf27392	CVE-2017-3167 CVE-2017-3169 CVE-2017-7659 CVE-2017-7668 CVE-2017-7679	The Apache vulnerabilities with Cisco UCS Manager identified by the Common Vulnerability and Exposures (CVE) IDs listed are fixed. The following related CVE ID does not affect Cisco UCS Manager because the use.htacess file and the <Limit/> directive in the configuration for httpd are not used in Cisco UCS Manager: • CVE-2017-9798

Release	Defect ID	CVE	Description
3.2(2b)	CSCvf16289	CVE-2015-8242	The vulnerability associated with a version of LibXML2 when used with Cisco UCS Manager has been fixed.
3.2(1d)	CSCvc88543	CVE-2016-0736 CVE-2016-2161 CVE-2016-5387 CVE-2016-8740 CVE-2016-8743	The vulnerabilities identified by one or more of the Common Vulnerability and Exposures (CVE) IDs listed do not impact any Cisco UCS Manager release. The following CVEs do not apply to Cisco UCS Manager because the relevant modules are not compiled as part of the Apache HTTP server used in Cisco UCS Manager: • CVE-2016-0736 • CVE-2016-2161 • CVE-2016-5387 • CVE-2016-8740 CVE-2016-8743 is applicable when backend servers are used. This functionality was added in Cisco UCS Manager Release 3.2(1). However, Release 3.2(1) also has the updated Apache version with the relevant fix for this vulnerability. Thus, this CVE also does not impact any Cisco UCS Manager release.

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 3.2(3p)

The following caveats are resolved in Release 3.2(3p):

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvt27869	In rare situations, on UCS 6200 Series Fabric Interconnect, the data sent from IOM were corrupted due to the corrupted parameter going out of bounds. This issue is resolved.	2.2(8f)A and C	3.2(3p)A and C
CSCvs97236	On detecting an uncorrectable ECC error, the CPU Integrated Memory Controller (iMC) patrol scrubber logs a truncated system address (4KB page boundary) to the machine check banks. Cisco UCS C460 M4 Rack Server translates the truncated memory address to a physical DIMM address. Depending on system population and configuration, the system event log (SEL) message logging the uncorrectable ECC error could point to a wrong DIMM. This issue is resolved.	3.2(3i)B	3.2(3p)B
CSCvu41110	Adaptive Double Device Data Correction (ADDDC), a memory RAS feature that enables dynamic mapping of failing DRAM, is now supported.	3.2(3a)B	3.2(3p)B

Resolved Caveats in Release 3.2(3o)

The following caveats are resolved in Release 3.2(3o):

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvo58565	The following drives running with N0A3 firmware, go offline and become temporarily unusable to the end customer: • Seagate HDD model ST1000NX0453 and ST2000NX0433 • Cisco PID UCS-HD1T7K12N and UCS-HD2T7K12N This issue does not have any impact to the data integrity of the drive. This issue is resolved	3.1(3c)C	3.2(3o)C
CSCvq76790	After firmware upgrade of Cisco IMC or Fabric Interconnect, the connectivity between Cisco IMC and Fabric Interconnect is lost due to a Physical Layer 1 issue or misconfiguration of port mode on the Fibre Channel port. This issue is resolved.	3.2(3g)A, 3.2(3j)A	3.2(3o)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvt55829	SanDisk Lightning II Solid State Drives (SSDs) LT0400MO and LT1600MO with respect to PIDS listed below, report 0 GB of available storage space remaining under normal operation at 40,000 power on hours. SSDs go offline and become unusable after power cycle event resulting in data loss, potentially on multiple drives if they are placed in service at the same time. The PIDs of affected SSDs are: • (400GB) UCS-SD400G1KHY-EP, UCS-SD400G12S4-EP, UCS-C3X60-12G240 • (1.6TB) UCS-SD16TG1KHY-EP, UCS-SD16TB12S4-EP, UCS-C3X60-12G2160 This issue is resolved.	3.2(1d)C	3.2(3o)C
CSCvm56662	When the following show command is run on Cisco UCS 6300 Series Fabric Interconnects, the system goes down and reboots. `show hardware internal bcm-usd info tables switch-cnt ing_service_counter_table all slot-num 0"` This issue is resolved.	3.2(3d)A, 3.2(3g)A	3.2(3o)A
CSCvm59040	Loss of network connectivity due to running out of memory after an uptime of over 180 days was sometimes encountered on hosts on Cisco standalone C-Series servers equipped with a VIC 1225 adapter. This issue is resolved.	3.2(3n)B and C	3.2(3o)B and C
CSCvo99427	When upgrading Cisco UCS Central to Release 2.0(1h), visibility to some UCS domains was lost. When running a connectivity test from Cisco UCS Central to the Cisco UCS Manager domains that lost visibility, the connection was successful but showed a warning message. This issue has been resolved.	3.1(1a)C	3.2(3o)C
CSCvp71363	In a system where a UCS C240 M5 server with a VIC 1457 adapter is managed by Cisco UCS Manager through a direct connect integration with UCS Fabric Interconnects, the following fault is displayed on unused or unconnected ports: `Adapter uplink interface x/y/z link state: unavailable. Please verify connectivity to Fabric Interconnect. Acknowledging FEX might be required.`	3.2(3a)A	3.2(3o)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvr91399	The following BIOS tokens are reset to Platform Default when they are pushed from Cisco UCS Central to UCS Manager. • SelectMemoryRASConfiguration • LocalX2Apic • BMEDMAMitigation	3.2(1d)A	3.2(3o)A

Resolved Caveats in Release 3.2(3n)

The following caveats are resolved in Release 3.2(3n):

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvq92352	In the very rare circumstance when a message with a corrupted length field from an attached FEX was received by the Fabric Interconnect `fwm` process, a Fabric Interconnect reboot was triggered. This issue is resolved.	2.2(8f)A	3.2(3n)A
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.	3.2(3h)A	3.2(3n)A
CSCvr06387	The SNMP process on the UCS 6324 Fabric Interconnect crashed repeatedly. This issue is resolved.	3.2(3a)A	3.2(3n)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.	3.2(3k)C	3.2(3n)C
CSCvm70115	When using a UCS server with a Hynix 32GB DDR4-2666-MHz RDIMM/PC4-21300/dual rank/x4/1.2v (18nm) - Revision 0 memory, the memory status appeared as "identity-unestablishable" in Cisco UCS Manager. This issue is resolved.	3.2(3j)A	3.2(3n)A

Resolved Caveats in Release 3.2(3l)

The following caveats are resolved in Release 3.2(3l):

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvh87378	Servers in community VLAN were not able to communicate with the primary VLAN after upgrade to UCS Manager version 3.1(3) or above when the server on the primary VLAN is inside the UCS domain. This issue is resolved.	3.2(2b)A	3.2(3l)A
CSCvj91628	Filesystems on the LSI 9271 RAID controller went offline or disconnected in some circumstances. This issue is resolved.	3.2(2b)C	3.2(3l)C
CSCvq57969	The Qualys vulnerability scanner did not recognize the HTTP security header as valid. This issue is resolved.	3.0(4a)B and C	3.2(3l)B and C
CSCvj81831	Board controller activation failed for C240-M5SX and C220-M5SX servers on attempting to downgrade to a major version when an upgraded BMC is present. This issue is resolved.	3.1(3a)C	3.2(3l)C

CSCvq04583	After upgrading Cisco UCS Manager to Release 3.2(3k) and decommissioning or re-acknowledging the UCS B230 M2 server, the server failed discovery. Error messages that were similar to the following were seen:
	`F16520 FSM:STAGE:FAILED]: Identify pre-boot environment agent on server X/Y(FSM-STAGE:sam:dme:ComputeBladeDiscover:PnuOSIdent)`
	`F999560[FSM:FAILED]: blade discovery X/Y(FSM:sam:dme:ComputeBladeDiscover). Remote-Invocation-Error: FSM Retries Exhausted`
	This issue is resolved. The blade server now gets discovered successfully after upgrading Cisco UCS Manager to Release 3.2(3l).
		3.2(3k)A	3.2(3l)A

Resolved Caveats in Release 3.2(3k)

The following caveats are resolved in Release 3.2(3k):

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvm89871	Under certain configuration sequences, Cisco UCS Manager managed Blade Servers failed discovery on Fabric Interconnect 6332 and 6332-16UP. The Tx transmit counter connected to the rack server FI port fails to increment. This issue is resolved.	3.1(2c)A	3.2(3k)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvn77413	Ethernet ports on a Series 6300 Fabric Interconnect showed a large number of VLAN drops on the discard counter, but with no appreciable performance impact. This issue is now resolved.	3.2(3h)A	3.2(3k)A
CSCvm55258	Under some circumstances, usually when updating a storage component, Cisco Hyperflex and C-series M5 server service profile association took 1 to 2 hours to perform the step "Perform Inventory of Server - PNUOS Inventory". This issue is resolved.	3.2(3b)A	3.2(3k)A
CSCvn72558	Cisco M2 Blade Servers were reporting invalid temperature sensor readings to the IOM, causing the IOM to throw a fault for critical thermal events, and spin up the fans as a safety measure. This issue is now resolved.	3.2(2d)A	3.2(3k)A
CSCvh07445	Under heavy traffic, Cisco B200 M5 blade servers failed discovery and showed `DME Logs: Remote-Invocation-Error: CimcVMedia Error: Error retrieving vmedia attributes list-MC Error(-6): Connection is closing` This issue is now resolved.	3.2(1d)A	3.2(3k)A
CSCvi26526	B200 M5 Blade Servers, as well as Hyperflex servers, would display a false warning of low memory when the kernel actually has free memory, but has allocated the memory in reusable system cache memory that is reclaimed on demand. This issue is now resolved.	3.2(2b)B	3.2(3k)B
CSCvn81327	The Cisco UCS-IOM-2304 IO Module crashed and produced a kernel core dump pointing to `pick_next_task_rt` in certain situations. The Linux kernel was patched to add a `dmesg` log to provide additional log information with kernel log files. Additionally, the kernel will now reboot after the core dump has been written to the flash memory. This additional data in the kernel core dump may help in determining the reason for the original kernel core.	3.2(2d)A	3.2(3k)A
CSCvn71713	UCS-FI-6296UP Blade Servers were undergoing shallow discovery and crashing with a core dump. This issue is now resolved.	3.2(3g))A	3.2(3k)A

Resolved Caveats in Release 3.2(3j)

The following caveats are resolved in Release 3.2(3j):

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvm95801 CSCvn01215	On UCS 6300 Series and UCS 6324, FI management IP address changes do not get updated in the IOM or FEX. Hence, the devices connected to the host interfaces continue to receive the old management IP address through the CDP process. This issue is resolved. The devices connected to the host interfaces now receive the updated management IP address through the CDP process.	3.2(3b)A	4.0(1d)A and 3.2(3j)A
CSCvn25191	In scenarios with very specific write/read patterns, there could be potential data loss for 3.8 TB and 7.6 TB Micron 5100 SSD SATA drives. UECC read errors and reallocated sector counts are displayed in SMART log. This issue is now resolved.	3.2(3h)B and 3.2(3h)C	3.2(3j)B and 3.2(3j)C
CSCvh70412	Cisco UCS Manager displayed blade server discovery failure messages after port flaps on the link between IOM and FI. This issue is now resolved.	3.2(2b)A	3.2(3j)A
CSCvm81348	Cisco UCS Manager Data Management Engine (DME) no longer crashes due to mismatched adminvCon values passed by Cisco UCS Central for dynamic and static vNICs.	3.2(2f)A	3.2(3j)A
CSCvm66118	When a PSU with serial number LIT*xxxxxx* is inserted or reseated in a chassis connected to a UCS 6300 Series Fabric Interconnect, it may cause the Fabric Interconnect to report PSU fan faults. However, the PSU LED remains green and the PSU and the fans continue to work. This issue is now resolved.	3.2(2f)B	3.2(3j)B
CSCvk55423	Creating a SNMP user by filling in just the password and retaining default values for all other fields was creating a user with AuthType as "md5" and AES as "False". This was an unsupported combination and a Major Fault was raised stating the reason of failed user creation. This issue is now resolved.	3.2(3d)A	3.2(3j)A

Resolved Caveats in Release 3.2(3i)

The following caveats are resolved in Release 3.2(3i):

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvj57615	In scenarios such as FI reboot during UCS Infrastructure Upgrade, mgmt0 IP may not appear in the **`show ip interface brief vrf management`** or **`show run interface mgmt0`** command from connect NX-OS. This issue is now resolved.	3.2(3d)A	3.2(3i)A
CSCvm68038	After the tech support logs are downloaded, samdme user sessions do not get cleared from the subordinate FI. This leads to multiple unresponsive sessions, and after the session count on the subordinate FI reaches 64 (maximum allowed), remote access to the FI is lost. This issue has been resolved. The samdme user sessions are automatically cleared from the subordinate FI after the techsuport logs are downloaded.	3.2(2d)A	3.2(3i)A
CSCvm21299	Primary FI upgrade no longer becomes unresponsive when logs are continuously written to the pa_setup.log file.	3.2(3a)A	3.2(3i)A
CSCvm54628	FI management IP address changes do not get updated in the IOM or FEX. Hence, the devices connected to the host interfaces continue to receive the old management IP address through the CDP process. This issue is resolved. The devices connected to the host interfaces now receive the updated management IP address through the CDP process.	3.2(3b)A	3.2(3i)A
CSCvk63036	Unable to form a SAN port-channel between a Cisco UCS Fabric Interconnect pair and a Cisco Fibre Channel switch, where the Organizationally Unique ID (OUI) of the switch is one of the following: • 003a9c • 000831 • d0a5a6 This issue is resolved.	3.2(3d)A	3.2(3i)A

CSCvm50159	In UCS-FI-6248UP, fans do not get detected by the switch. As a result, the switches shut down with a series of error messages:
	`System minor alarm on fans: One fan missing or failed`
	`Fan module 1 xxxx-FAN removed`
	`System shutdown in 60 seconds due to fan removal`
	`System major alarm on fans: Multiple fans missing or`
	`failed`
	`System shutdown in 55 seconds due to fan removal`
	`System shutdown in 50 seconds due to fan removal`
	This issue is resolved.
		2.2(8m)A	3.2(3i)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvm08604	During chassis firmware upgrade on Cisco S3260 chassis, the security keys for the Self-Encrypting Drives (SEDs) are no longer mismatched between the controller and the drives.	3.2(3b)A	3.2(3i)A
CSCvm91294	In a UCS FI setup connected to S3260 chassis with the following conditions, the DME process crashes after upgrading the chassis firmware: • servers having UCS-C3K-M4 RAID storage controllers and rear boot SSDs • disk zoned to both the controllers, and VDs created on top loading disks and rear boot SSDs This issue is resolved.	3.2(3g)A	3.2(3i)A
CSCvm07945	ASPM was enabled by default on standalone and UCS Manager-managed C460 M4 servers. ASPM transitions were resulting in system crashes on these servers. This issue is resolved. ASPM is now disabled by default and is not user configurable.	3.2(3a)B and C	3.2(3i)B and C
CSCvm09239	In a setup where aUCS 2304 IOM is connected to a UCS 6300 Series FI through a single link with a 40G QSFP cable, the IOMs no longer disconnect and reconnect while gathering chassis log files from UCS Central.	3.2(3d)A	3.2(3i)A
CSCvk63025	UCS 6332-16UP port 33/34 no longer has connectivity issues with C93180YC-FX port 49/50 when using a CU1M passive cable.	3.2(3b)A	3.2(3i)A
CSCvf97761	Left-click does not highlight any item in the Navigation pane. However, the item details are displayed in the Work pane. This issue is resolved	3.1(3a)B	3.2(3i)B
CSCvm44391	The vNIC template lists duplicate vLAN entries from **LAN Cloud** and **Appliance** options. This issue is resolved. The vNIC template now filters vLAN entries and lists only unique vLAN names.	3.2(3g)A	3.2(3i)A
CSCvm11482	With Windows 2019 WHLK test kits, UCS M4 BIOS was failing the "SmBIOS Table Specific Requirement" test with errors such as: `non-printable characters found in SmBIOS table structure` This issue is resolved.	4.0(1a)B	3.2(3i)B

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvm57553	On a very small number of UCS-IOM-2304, the boot and run time may become degraded due to JFFS2 Clearmarker filesystem errors. This is caused by a limitation in a vendor-specific kernel filesystem patch, and affects IOMs that are built with 16-3743-01 NOR flash chips. This issue is resolved, and no longer affects any UCS IOM.	4.0(1a)A	3.2(3i)A

Resolved Caveats in Release 3.2(3h)

The following caveats are resolved in Release 3.2(3h):

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvj63703	Activation of the UCSC-SAS-M5 or UCSC-SAS-M5HD storage controller no longer fails when you try to downgrade the storage controller firmware image from a higher version to a version in the 3.2(3) C-Bundle. This issue applies to any C220 M5, C240 M5, or C480 M5 server with UCSC-SAS-M5/UCSC-SAS-M5HD storage controllers.	3.2(3a)C	3.2(3h)C
CSCvj10772	In a UCS Mini setup with the following conditions multi-cast traffic no longer is dropped on the server side: • IP IGMP snooping is enabled • vEthernets bound to different port-channels are registered to some multi-cast groups • One of the port-channel is deleted or goes down	3.0(1c)A	3.2(3h)A
CSCvi80895	After upgrading Cisco UCS Manager to Release 3.2(2c), TACAC users are able to create full local backup of Cisco UCS Manager.	3.2(2b)A	3.2(3h)A
CSCvk36317	After upgrading Cisco UCS Manager from Release 3.1(1l) to 3.2(3b), the existing PVLAN configuration no longer fails. The upstream server in the primary VLAN is now able to reach the VM/Host in the isolated VLAN in the UCS domain.	3.2(3a)A	3.2(3h)A
CSCvk40744	When a Cisco UCS C240 M4 Server is associated with a service profile, the service profile does not implement the Core Multiprocessing BIOS token to the server using UCSM BIOS policy. The service profile always configures Core Multiprocessing token value as the default value (**All**) even if a different value is set in the BIOS policy. This issue is now resolved.	3.2(3a)A	3.2(3h)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvj45253	In a setup with Cisco UCS B200 M5 Server or Cisco UCS B480 M5 Server, sometimes the FlexFlash Controller is not detected. This is caused due to command timeout. This issue is now resolved.	3.2(2b)A	3.2(3h)A
CSCvj78742	The active IOM no longer reboots unexpectedly due to satsyslog hap reset while failing over from peer IOM that was rebooted.	3.2(3d)A	3.2(3h)A
CSCvk65195	Cisco UCS B480 M5 Servers with BIOS version B480M5.3.2.3f.0.0523181557 and earlier reported incorrect power usage. This incorrect reporting could cause a chassis outage when a UCS 5108 chassis crossed the threshold of maximum power usage. This issue is now resolved.	3.2(3g)	3.2(3h)A
CSCvk48744	In UCS blade servers, Serial Over LAN (SOL) and IPMI policies work as per design.	3.2(3a)A	3.2(3h)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. This issue is now resolved.	3.1(2c)A	3.2(3h)A
CSCvh66141	KVM log in does not fail when you use non-native authentication domain and without logging in Cisco UCS Manager first.	3.1(3a)A	3.2(3h)A
CSCvk51589	Cisco Fabric Interconnect reboots with the following message: `Reset triggered due to HA policy of Reset` No VIM process core is seen. This issue is now resolved.	3.2(2d)A	3.2(3h)A
CSCvj74285	Cisco IMC reboots due to Out of memory (OOM) that may occur on M5 servers with firmware version 3.1(3a). Cisco IMC is not accessible over a network. This issue is now resolved.	3.2(3a)C	3.2(3h)C
CSCvk71319	VIM process core causes FI reboot. This issue is now resolved.	3.2(3g)A	3.2(3h)A

Resolved Caveats in Release 3.2(3g)

The following caveats are resolved in Release 3.2(3g):

Defect ID	Description	First Bundle Affected	Resolved in Release
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 3.2(3g) prevents this issue from occurring.	3.2(2b)A	3.2(3g)A
CSCvj91316	When running Cisco UCS Manager 3.2(2b) with Cisco UCS 2304 IOM/FEX, the FEX no longer corrupts TX frames on the Network Facing port (NIF).	3.2(2b)A	3.2(3g)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

Resolved Caveats in Release 3.2(3e)

The following caveats are resolved in Release 3.2(3e):

Defect ID	Description	First Bundle Affected	Resolved in Release
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	3.2(3e)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	3.2(3e)B
CSCvj22874	FC traffic was affected, and fcpio_data_cnt_mismatch errors appeared in the adapter. This happened under the following conditions: • When using 6332-16UP FIs. • When the FI was receiving Ethernet frames that were larger than the configured MTU size. This resulted in stomped CRC errors in the IOM and adapter. • When the jumbo frames and FC traffic went out of same server port towards the IOM. This issue is now resolved.	3.1(3c)A	3.2(3e)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvi06412	A server part of Cisco UCS Mini in VLAN 1 had intermittent access issues to only a few hosts in the same VLAN, but worked for other hosts in the same VLAN. This issue occurred when one or both of the backplane ports between the FI and the server's adapter were not programmed correctly for VLAN 1. This issue has been resolved.	3.1(2f)A	3.2(3e)A

Resolved Caveats in Release 3.2(3d)

The following caveats are resolved in Release 3.2(3d):

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvj08442	After adding the secondary FI to the cluster, the FI no longer fails to configure FC ports in FC switching mode.	3.2(2b)A	3.2(3d)A
CSCvj46999	VLAN addition or removal on the border port caused some pinned vNICs to temporarily flap and recover on their own in a few seconds. This happened when the following conditions were met: • Total number of VLANs on the border port before adding or removing a VLAN was more than 980 • Number of VLAN ranges was more than 512 **Note** This condition is specific to the number of VLAN ranges, not the number of VLANs. This issue is now resolved.	3.1(3c)A	3.2(3d)A
CSCvj50398	During UCS Infrastructure upgrades to Cisco UCS Manager Release 3.2(3a) or 3.2(3b) from any previous release, Cisco UCS servers no longer reboot unexpectedly without user acknowledgement in any of the following scenarios: • If the C Series bundle being used is earlier than Release 3.1(2) • If the B Series bundle has the Asset Tag value configured	3.2(3a)A 3.2(3b)A	3.2(3d)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvj48557	In Cisco UCS systems running Cisco UCS Manager Release 3.2(3a) or 3.2(3b), Cisco UCS servers no longer reboot unexpectedly without user acknowledgement in any of the following scenarios: • Any change is made in the existing service profile for the first time after the upgrade • An intentional change is made to the Asset Tag value in the service profile • Cisco UCS Manager is downgraded	3.2(3a)A 3.2(3b)A	3.2(3d)A
CSCvj32984	Operating System logs had a large amount of persistent SCSI abort commands for FCID 0xffffffff. Operating Systems utilizing remote FC / FCoE storage may hang. This happened when there was significant Fibre Channel (FC)/Fibre Channel over Ethernet (FCoE) traffic, and affected the following VIC adapters: • Cisco UCS VIC 1340 modular LOM (UCSB-MLOM-40G-03) • Cisco UCS VIC 1380 mezzanine adapter (UCS-VIC-M83-8P) • Cisco UCS VIC 1385 Dual Port 40Gb QSFP+ CAN (UCSC-PCIE-C40Q-03) • Cisco UCS VIC 1387 Dual Port 40Gb QSFP CNA MLOM (UCSC-MLOM-C40Q-03) This issue has been resolved.	3.2(3a)B, 3.2(3a)C 3.2(3b)B, 3.2(3b)C	3.2(3d)B, 3.2(3d)C
CSCvh75430	On a Cisco UCS Manager 3.2(2) system configured with **Allowed SSL protocols** set to **Only TLS 1.2**, the Cisco UCS KVM Direct login page no longer allows TLS version 1.0 on Out of Band (OOB) addresses.	3.2(2b)A	3.2(3d)A

Resolved Caveats in Release 3.2(3b)

The following caveats are resolved in Release 3.2(3b):

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvi57046	The FC-MAC defect no longer causes the following behavior on 6332-16UP fabric interconnects running Cisco UCS Manager Release 3.2(1x) or 3.2(2x): Bringing up fc 1/3 will impact fc 1/4 if it is already up Bringing up fc 1/4 will impact fc 1/7 if it is already up Bringing up fc 1/10 will impact fc 1/11 if it is already up	3.2(2d)A	3.2(3b)A
CSCvi50985	On Cisco UCS Manager Release 3.1(3a) or later releases, blade server discovery no longer fails when the blade server has a Warp Drive (UCSB-F-LSI-400S) installed.	3.1(3a)A	3.2(3b)A
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	3.2(3b)A
CSCvi26150	When using UCSB-PSU-2500ACDV with Grid or N+1 power policy in Cisco UCS Manager Releases 3.2(2b) or 3.2(2d), Cisco UCS Manager no longer reports incorrect wattage.	3.2(2b)B	3.2(3b)B

CSCvj03597	Updating the BIOS on UCS B480 M5 blade servers no longer fails with the following status:
	`UCSM FSM status:`
	`        Remote Result: End Point Failed`
	`        Remote Error Code: ERR UPDATE Failed`
	`        Remote Error Description: Flash write failed. Flash on server appears to be bad.`
	`        Status: Associate Fail`
	`        Previous Status: Associate Fail`
	`        Timestamp: <time-stamp>`
	
	`        Progress (%): <%>`
	`        Current Task: Waiting for BIOS update to complete(FSM-STAGE:sam:dme:ComputePhysicalAssociate:PollBiosUpdateStatus)`
		3.2(2b)B	3.2(3b)B

CSCvj01763	While upgrading Cisco UCS Manager to Release 3.2(3a), dynamic vNICs/VFs were not created on servers with VIC 12XX based adapters. This issue is now resolved.	3.2(3a)A	3.2(3b)A

Resolved Caveats in Release 3.2(3a)

The following caveats are resolved in Release 3.2(3a):

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvg21234	The Matrox display driver now loads correctly and works successfully on all M4 EP blade servers with Windows Server 2016.	3.1(3c)B	3.2(3a)B
CSCvh81553	UCS S3260 M4 servers in an S3260 chassis integrated with Cisco UCS Manager no longer fail discovery after upgrade from Cisco UCS Manager Release 3.1(3c) to 3.2(2d).	3.2(2d)C	3.2(3a)C
CSCvf15927	The Matrox display driver now loads correctly and works successfully on B260 and B460 M4 blade servers with Windows Server 2016.	3.2(1d)B	3.2(3a)B
CSCvf40571	Service profile association failed after FI failover from FI A to FI B and the Associate FSM remained at **ComputePhysicalAssociateSwConfigHostOSPeer** under the following conditions: • It is a High Availability setup with the server discovered from both ends (connection status: A, B) • The server is associated and powered off • The FI, which is the managing instance of the adaptor(s) on this server, is brought offline This issue is now resolved.	3.1(1h)A	3.2(3a)A
CSCvh04298	The IOMs connected to an FI no longer reboot unexpectedly due to software-controlled resets.	3.1(3d)A	3.2(3a)A
CSCvg06395	While configuring RAID60 virtual drives on a Cisco UCS S3260 setup, Cisco UCS Manager no longer displays an "Insufficient disks for the specified RAID level" configuration failure error when there is enough space left in existing disk groups.	3.2(2b)C	3.2(3a)C
CSCvh76070	UCS B200 M5 servers no longer have connectivity issues with SD cards.	3.2(2b)B	3.2(3a)B
CSCvf53118	While changing the FI mode from Ethernet Switching mode to End-Host mode, the pending user-acknowledgment is now displayed, and the FI reboots only after the FI reboot notification is acknowledged.	3.2(1d)A	3.2(3a)A
CSCvh22485	In a VMFEX setup with PVLAN host configurations on the Veths, after vMotion or VM migration, VMs were unable to receive broadcast or multicast packets, including ARP packets. This issue has been resolved.	3.2(1d)A	3.2(3a)A

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvf26570	When the `/var/sysmgr` partition becomes completely full, the fault for the sysmgr space being full is reported. After the disk space is recovered, logging restarts automatically without pmon restart.	3.1(1g)A	3.2(3a)A
CSCvf51664 CSCvg08158	Multicast data traffic received on the FI uplink with secondary VLAN no longer gets dropped because the Designated Receiver (DR) for the Primary and Secondary VLANs will always be the same, irrespective of the number of uplinks present.	3.2(2b)A	3.2(3a)A
CSCvg92817	Upgrading to Cisco UCS Manager Release 3.2 with the power policy set to Grid Power no longer generates any redundancy power lost messages when the right number of power supplies are present and active to satisfy the Grid Power policy.	3.2(1d)B	3.2(3a)B
CSCvf91309	When disassociating a service profile in Cisco UCS Manager, the underlying NX-OS vEthernet configuration is now cleared.	2.5(1a)A	3.2(3a)A
CSCvg31345	Copying debug plugins or any infrastructure image files to the subordinate FI no longer fails.	2.2(8c)A	3.2(3a)A
CSCvg16805	In a setup with a 6332-16UP FI, a 5108 blade chassis, and IOM 2304, with one 40G link from IOM to FI, request for a chassis techsupport no longer brings down the subordinate IOM.	3.1(1h)A	3.2(3a)A
CSCvh55047	In a system with UCS M5 servers and UEFI SAN boot policy, bladeAG cores are no longer generated.	3.2(1d)A	3.2(3a)A
CSCvg64592	Rack servers integrated with FIs did not have connectivity after reboot of the subordinate FI, if the VLAN range exceeded 255 characters. This issue has been resolved.	3.1(3c)A	3.2(3a)A
CSCvg11168	On large scale setups, the secondary FI (B) no longer crashes after the following sequence of events: • Decommission/recommission servers • Change cluster lead • Collect UCSM tech-support logs from console: FI:A	3.2(2b)A	3.2(3a)A
CSCvh87013	BIOS tokens for CPU performance in M5 rack servers no longer take incorrect values for HPC and Enterprise settings.	3.1(3a)C	3.2(3a)
CSCvg75210	Storage RAID controller firmware upgrade no longer fails due to storage PCI addresss mismatch in PNUOS and in MO.	3.2(2b)A	3.2(3a)

Resolved Caveats in Release 3.2(2f)

The following caveats are resolved in Release 3.2(2f)

Table 15: Resolved Caveats in Release 3.2(2f)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvh32617	UCS B480 M5 blade servers that are fully loaded with 48*128G DIMMs and UCS-CPU-8176M no longer fail discovery.	3.2(2b)A	3.2(2f)A
CSCvh55047	In a system with UCS M5 servers and UEFI SAN boot policy, bladeAG cores are no longer generated.	3.2(1d)A	3.2(2f)A
CSCvh64120	DME no longer crashes after an upgrade to Cisco UCS Manager Release 3.1(3) or Release 3.2(2).	3.1(3a)A	3.2(2f)A
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	3.2(2f)A
CSCvi06930	Discovery of UCSC-C480-M5 through Cisco UCS Manager no longer fails when more than 10 NVMe drives are populated.	3.2(2b)A	3.2(2f)A
CSCuy98678	Cisco UCS 6296 Fabric Interconnect no longer crashes unexpectedly with kernel panic, and impacts any devices connected the Fabric Interconnect.	2.2(6c)A	3.2(2f)A

Resolved Caveats in Release 3.2(2d)

The following caveats are resolved in Release 3.2(2d)

Table 16: Resolved Caveats in Release 3.2(2d)

Defect ID	Description	First Bundle Affected	Resolved in Release
CSCvg62341	OS driver information is properly displayed after upgrading or downgrading Cisco IMC.	3.1(2b)C	3.2(2d)C
CSCvg74318	Cisco UCS Manager no longer generates a fault for a fan module that is not installed on the C240 M5.	3.1(2b)C	3.2(2d)C
CSCvg78583	Cisco UCS Manager now displays local disk catalog details on the C240 M5.	3.2(2b)C	3.2(2d)C
CSCvh00935	Cisco IMC no longer falsely reports a hard disk drive temperature as hot.	3.2(2b)A	3.2(2d)A
CSCvg93195	An IOM thermal core on a 3GFI setup no longer occurs.	3.2(2b)B	3.2(2d)B
CSCvh02465	Cisco UCS Manager now displays the physical location of the NVME drive.	3.2(2b)A	3.2(2d)A

Resolved Caveats in Release 3.2(2c)

The following caveats are resolved in Release 3.2(2c):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvf89931	Broadcom SAS IT controller firmware now initializes the I2C interface correctly and no longer results in the link between the BMC and the controller going down.	3.2(1d)C	3.2(2c)C
CSCvg50400	While upgrading firmware when there is heavy I2C traffic,the storage controller firmware no longer hits exceptions that cause firmware download failures.	3.2(2b)C	3.2(2c)C
CSCvg52570	When using VIC Firmware version 4.2(2a) with Cisco UCS Manager Release 3.2(2b) and UCS C-Series Software Release 3.1(2b), FCoE performance no longer drops with workloads involving IO sizes less than 32K.	3.2(2b)B	3.2(2c)B
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)B	3.2(2c)B
CSCvg50989	ESXi 6.5 installation no longer fails on SD cards with UCS M5 servers or HX servers.	3.2(2b)B	3.2(2c)B

Resolved Caveats in Release 3.2(2b)

The following caveats are resolved in Release 3.2(2b):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvf23628	Cisco UCS B200 M5 Blade Server no longer fails VSAN certification in All flash configurations with SATA SSDs.	3.2(1d)B	3.2(2b)B
CSCve47615	In Release 3.2(1d), the **TPM Clear** operation initiated through Cisco UCS Manager did not clear the TPM module. This has now been resolved. The **TPM Clear** operation initiated through Cisco UCS Manager clears the TPM module.	3.2(1d)B	3.2(2b)B
CSCve49653	When TXT is enabled from Cisco UCS Manager BIOS policy, the system no longer fails to power on.	3.2(1d)B	3.2(2b)B

Resolved Caveats in Release 3.2(1d)

The following caveats are resolved in Release 3.2(1d):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCve34690	FlexFlash SD storage no longer fails with a missing fault.	3.1(2b)A	3.2(1d)A
CSCve34055	The Fabric Interconnect no longer reboots due to a CDP process crash.	3.1(2f)A	3.2(1d)A
CSCvd78110	After upgrading Cisco UCS Manager from release 2.2(6e) to Release 3.1(2e), Cisco UCS Manager no longer incorrectly configures the uplink port-channel speed as 10G instead of the previously configured 1G speed.	3.1(2e)A	3.2(1d)A
CSCve34167	When Call Home with Call Home message throttling was enabled in Cisco UCS Manager, no call home messages were sent although no errors were generated. This issue is now resolved.	3.1(2e)A	3.2(1d)A
CSCve15822	In some cases, when the semaphore to shared memory dropped to 0 and mcserver was able to get past cmclog_setlevel(), Cisco UCS Manager was unable to respond to CMC. This issue is now resolved.	3.1(2f)A	3.2(1d)A

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 3.2(3o)

The following caveats are open in Release 3.2(3o):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvv80576	On a UCS Managed B or C Series server or UCS Mini connected to either 6200 Series or 6300 Series Fabric Interconnects, after a vNIC fail-over, traffic does not switch to the second Fabric Interconnect, resulting in dropped traffic. Servers with 6400 Series Fabric Interconnects are not affected.	Make sure there is continuous traffic from the vNIC source during fail-over.	3.2(3o)A

Open Caveats for Release 3.2(3k)

The following caveats are open in Release 3.2(3k):

Defect ID	Symptom	Workaround	First Bundle Affected

CSCvq04583	After upgrading Cisco UCS Manager to Release 3.2(3k) and decommissioning or re-acknowledging the UCS B230 M2 server, the server fails discovery. Error messages that are similar to the following are seen:
	`F16520 FSM:STAGE:FAILED]: Identify pre-boot environment agent on server X/Y(FSM-STAGE:sam:dme:ComputeBladeDiscover:PnuOSIdent)`
	`F999560[FSM:FAILED]: blade discovery X/Y(FSM:sam:dme:ComputeBladeDiscover). Remote-Invocation-Error: FSM Retries Exhausted`
		If this happens, downgrade the Cisco UCS Manager version to any version earlier than Release 3.2(3k).	3.2(3k)A
			Resolved in 3.2(3l)A

Open Caveats for Release 3.2(3h)

The following caveats are open in Release 3.2(3h):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvn25191	In scenarios with very specific write/read patterns, there could be potential data loss for 3.8 TB and 7.6 TB Micron 5100 SSD SATA drives. UECC read errors and reallocated sector counts are displayed in SMART log.	For 3.8 TB drives, upgrade firmware to D0MU427. For 7.6 TB, upgrade firmware to D0MU827.	3.2(3h)B and 3.2(3h)C Resolved in 3.2(3j)B and 3.2(3j)C

Open Caveats for Release 3.2(3g)

The following caveats are open in Release 3.2(3g):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvk65195	Cisco UCS B480 M5 Servers report incorrect power usage, which could potentially cause a chassis outage when a UCS 5108 chassis crosses the threshold of maximum power usage. This issue occurs in Cisco UCS B480 M5 Servers with BIOS version B480M5.3.2.3f.0.0523181557 and earlier.	Configure blade level power capping with a value 40% lower than the actual desired value for Cisco UCS B480 M5 Servers.	3.2(3g) Resolved in 3.2(3h)
CSCvk71319	VIM process core causes FI reboot.	There is no known workaround.	3.2(3g) Resolved in 3.2(3h)
CSCvm44391	vNIC template lists duplicate vLAN entries from **LAN Cloud** and **Appliance**.	Disable Org permissions on LAN Cloud Global Policy.	3.2(3g)A Resolved in 3.2(3i)A
CSCvm91294	In a UCS FI setup connected to S3260 chassis with the following conditions, the DME process crashes after upgrading the chassis firmware: • servers having UCS-C3K-M4 RAID storage controllers and rear boot SSDs • disk zoned to both the controllers, and VDs created on top loading disks and rear boot SSDs	No known workaround.	3.2(3g)A Resolved in 3.2(3i)A
CSCvn71713	UCS-FI-6296UP blade servers undergo shallow discovery and crashing with a core dump.	None	3.2(3g)A Resolved in 3.2(3k)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvo59242	On UCS Mini only, two MAC addresses are unable to communicate between 6300 Series Fabric Interconnects. Communication with gateway ports or any other northbound traffic is unaffected for either MAC address. This seems to occur when there is a active MAC entry on a Fabric Interconnect, even though the MAC has moved to the peer FI. This will occur when the adjacency bit (`adj`) is set on the initial FI, before the MAC move. **`Show mac address-table`** can confirm that the MAC is present on both the FIs. Use the following command as a simple check for the condition: **`Show hardware internal libsdk mtc l2 mac-table-ce | grep '1 1 0 0 1 1 0'`** **`Show hardware internal libsdk mtc l2 mac-table-ce | grep '1 1 0 0 0 1 0'`** If it returns a match for the first or second string, the `adj` bit is set (incorrectly), and the MAC address is still being learned on the current FI. The issue is present, but connectivity problems will not occur until the MAC moves to the peer FI.	As a workaround, configure the MAC as a static MAC, and then delete the static MAC entry.	3.2(3g)A
	Despite the locale being defined on a sub-organization, remotely authenticated users can see all the organizations.	None	3.2(3g)A Resolved in 4.0(2e)A
CSCvn82697	Despite the locale being defined on a sub-organization, remotely authenticated users can see all the organizations.	None	3.2(3g)A Resolved in 4.0(2e)A

Open Caveats for Release 3.2(3d)

The following caveats are open in Release 3.2(3d):

Defect ID	Symptom	Workaround	First Bundle Affected

CSCvj57615	In scenarios such as FI reboot during UCS Infrastructure Upgrade, mgmt0 IP may not appear in the command **`show ip interface brief vrf management`** or **`show run interface mgmt0`** from connect NX-OS.	Change the IP address of the affected fabric interconnect through the Cisco UCS Manager GUI or CLI to a different IP address and then change the IP address back to the original IP.
		Alternatively, contact Cisco TAC to update the mgmt0 IP address.
		Also, rebooting the FI may 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 the mgmt0 IP address is assigned using:
		`connect nx a/b`
		`show ip interface brief vrf management`
			3.2(3d)A
			Resolved in 3.2(3i)A

CSCvk63036	Unable to form a SAN port-channel or trunking between a Cisco UCS Fabric Interconnect pair and a Cisco Fibre Channel switch, where the Organizationally Unique ID (OUI) of the switch is one of the following: • 003a9c • 000831 • d0a5a6	Use single F-Port links (Trunk mode should be OFF for UCS FI and MDS)	3.2(3d)A Resolved in 3.2(3i)A
CSCvm09239	In a setup where a UCS 2304 IOM is connected to a UCS 6300 FI series with a 40G QSFP cable, the IOMs disconnect and reconnect while gathering chassis log files from UCS Central	No known workaround	3.2(3d)A Resolved in 3.2(3i)A
CSCvj78742	The active IOM longer reboots unexpectedly due to satsyslog hap reset while failing over from peer IOM that was rebooted.	Ensure that LLDP is disabled on vNICs and vHBAs.	3.2(3d)A Resolved in 3.2(3h)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvk55423	Creating a SNMP user by filling in just the password and retaining default values for all other fields creates a user with AuthType as "md5" and AES as "False". This is an unsupported combination and a Major Fault is raised stating the reason of failed user creation.	Select Auth type as "SHA" and AES as "True" while creating an SNMP user.	3.2(3d)A Resolved in 3.2(3j)A

Open Caveats for Release 3.2(3b)

The following caveats are open in Release 3.2(3b):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvj32984	Operating System logs have a large amount of persistent SCSI abort commands for FCID 0xffffffff. Operating Systems utilizing remote FC / FCoE storage may hang. This happens when there is significant Fibre Channel (FC)/Fibre Channel over Ethernet (FCoE) traffic, and affects the following VIC adapters: • Cisco UCS VIC 1340 modular LOM (UCSB-MLOM-40G-03) • Cisco UCS VIC 1380 mezzanine adapter (UCS-VIC-M83-8P) • Cisco UCS VIC 1385 Dual Port 40Gb QSFP+ CAN (UCSC-PCIE-C40Q-03) • Cisco UCS VIC 1387 Dual Port 40Gb QSFP CNA MLOM (UCSC-MLOM-C40Q-03)	For Cisco UCS B-Series Servers and Integrated C-Series Rack-Mount Servers, downgrade the blade or rack firmware to a release prior to Cisco UCS Manager Release 3.2(3a) For Cisco UCS C-Series Standalone Rack-Mount Servers, downgrade the rack firmware to a release prior to Release 3.1(3a) For more information, see the Cisco Software Advisory at https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/SA/SW_Deferral_Notice_CSCvj32984_v3.html	3.2(3a)B, 3.2(3a)C 3.2(3b)B, 3.2(3b)C Resolved in 3.2(3d)B, 3.2(3d)C

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvj50398	During UCS Infrastructure upgrades to Cisco UCS Manager Release 3.2(3a) or 3.2(3b) from any previous release, Cisco UCS servers may reboot unexpectedly without user acknowledgement in any of the following scenarios: • If the C Series bundle being used is earlier than Release 3.1(2) • If the B Series bundle has the Asset Tag value configured	If already running Cisco UCS Manager Release 3.2(3a) or 3.2(3b), do not modify the Asset Tag. For UCS C-Series integrated with Cisco UCS Manager, there is no workaround to avoid encountering this issue during the upgrade of the UCS Infrastructure from UCS Manager 3.1(2) or earlier to an affected release. Upgrade to a patched release once available. For more information, see the Cisco Software Deferral Notice at https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/SA/SW_Deferral_Notice_CSCvj50398_v3.html	3.2(3a)A 3.2(3b)A Resolved in 3.2(3d)A
CSCvj48557	In Cisco UCS systems running Cisco UCS Manager Release 3.2(3a) or 3.2(3b), Cisco UCS servers may reboot unexpectedly without user acknowledgement in any of the following scenarios: • Any change is made in the existing service profile for the first time after the upgrade • An intentional change is made to the Asset Tag value in the service profile • Cisco UCS Manager is downgraded	If already running Cisco UCS Manager Release 3.2(3a) or 3.2(3b), do not modify the Asset Tag. For UCS C-Series integrated with Cisco UCS Manager, there is no workaround to avoid encountering this issue during the upgrade of the UCS Infrastructure from UCS Manager 3.1(2) or earlier to an affected release. Upgrade to a patched release once available. For more information, see the Cisco Software Deferral Notice at https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/SA/SW_Deferral_Notice_CSCvj50398_v3.html	3.2(3a)A 3.2(3b)A Resolved in 3.2(3d)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvm54628	FI management IP address changes do not get updated in the IOM or FEX. Hence, the devices connected to the host interfaces continue to receive the old management IP address through the CDP process.	Disable and then again enable CDP option in Cisco UCS Manager using Network Control Policy.	3.2(3b)A Resolved in 3.2(3i)A
CSCvk63025	UCS 6332-16UP port 33/34 no longer has connectivity issues with C93180YC-FX port 49/50 on CU1M passive cable.	No known workaround.	3.2(3b)A Resolved in 3.2(3i)A
CSCvm08604	During chassis firmware upgrade on Cisco S3260 chassis, the security keys for the Self-Encrypting Drives (SEDs) are mismatched between the controller and the drives.	Contact Cisco TAC for steps to synchronize the SED Keys and re-import drive configuration.	3.2(3b)A Resolved in 3.2(3i)A
CSCvm95801 CSCvn01215	On UCS 6300 Series and UCS 6324, FI management IP address changes do not get updated in the IOM or FEX. Hence, the devices connected to the host interfaces continue to receive the old management IP address through the CDP process.	Disable and then enable CDP option in Cisco UCS Manager using Network Control Policy.	3.2(3b)A Resolved in 4.0(1d)A and 3.2(3j)A
CSCvj91628	Filesystems on the LSI 9271 RAID controller go offline or disconnect. The LSI controller logs a fatal firmware error.	None. Reboot to recover.	3.2(3b)A Resolved in 3.2(3l)C

Open Caveats for Release 3.2(3a)

The following caveats are open in Release 3.2(3a):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvm21299	Primary FI upgrade becomes unresponsive at 98% with the following error message: `Pre-Upgrade check failed. Insufficient free space in /var/sysmgr. Less than required 20%.`	Delete /var/sysmgr/sam_logs/pa_setup.log file to clear the memory.	3.2(3a)A Resolved in 3.2(3i)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvj32984	Operating System logs have a large amount of persistent SCSI abort commands for FCID 0xffffffff. Operating Systems utilizing remote FC / FCoE storage may hang. This happens when there is significant Fibre Channel (FC)/Fibre Channel over Ethernet (FCoE) traffic, and affects the following VIC adapters: • Cisco UCS VIC 1340 modular LOM (UCSB-MLOM-40G-03) • Cisco UCS VIC 1380 mezzanine adapter (UCS-VIC-M83-8P) • Cisco UCS VIC 1385 Dual Port 40Gb QSFP+ CAN (UCSC-PCIE-C40Q-03) • Cisco UCS VIC 1387 Dual Port 40Gb QSFP CNA MLOM (UCSC-MLOM-C40Q-03)	For Cisco UCS B-Series Servers and Integrated C-Series Rack-Mount Servers, downgrade the blade or rack firmware to a release prior to Cisco UCS Manager Release 3.2(3a) For Cisco UCS C-Series Standalone Rack-Mount Servers, downgrade the rack firmware to a release prior to Release 3.1(3a) For more information, see the Cisco Software Advisory at https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/SA/SW_Deferral_Notice_CSCvj32984_v3.html	3.2(3a)B, 3.2(3a)C 3.2(3b)B, 3.2(3b)C Resolved in 3.2(3d)B, 3.2(3d)C
CSCvj63703	Activation of the UCSC-SAS-M5 or UCSC-SAS-M5HD storage controller could fail when you try to downgrade the storage controller firmware image from a higher version to a version in the 3.2(3) C-Bundle. This happens occurs in C220 M5, C240 M5, or C480 M5 server with UCSC-SAS-M5/UCSC-SAS-M5HD storage controllers.	There is no known workaround.	3.2(3a)C Resolved in 3.2(3h)C

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvj50398	During UCS Infrastructure upgrades to Cisco UCS Manager Release 3.2(3a) or 3.2(3b) from any previous release, Cisco UCS servers may reboot unexpectedly without user acknowledgement in any of the following scenarios: • If the C Series bundle being used is earlier than Release 3.1(2) • If the B Series bundle has the Asset Tag value configured	If already running Cisco UCS Manager Release 3.2(3a) or 3.2(3b), do not modify the Asset Tag. For UCS C-Series integrated with Cisco UCS Manager, there is no workaround to avoid encountering this issue during the upgrade of the UCS Infrastructure from UCS Manager 3.1(2) or earlier to an affected release. Upgrade to a patched release once available. For more information, see the Cisco Software Deferral Notice at https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/SA/SW_Deferral_Notice_CSCvj50398_v3.html	3.2(3a)A 3.2(3b)A Resolved in 3.2(3d)A
CSCvj48557	In Cisco UCS systems running Cisco UCS Manager Release 3.2(3a) or 3.2(3b), Cisco UCS servers may reboot unexpectedly without user acknowledgement in any of the following scenarios: • Any change is made in the existing service profile for the first time after the upgrade • An intentional change is made to the Asset Tag value in the service profile • Cisco UCS Manager is downgraded	If already running Cisco UCS Manager Release 3.2(3a) or 3.2(3b), do not modify the Asset Tag. For UCS C-Series integrated with Cisco UCS Manager, there is no workaround to avoid encountering this issue during the upgrade of the UCS Infrastructure from UCS Manager 3.1(2) or earlier to an affected release. Upgrade to a patched release once available. For more information, see the Cisco Software Deferral Notice at https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/SA/SW_Deferral_Notice_CSCvj50398_v3.html	3.2(3a)A 3.2(3b)A Resolved in 3.2(3d)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvh31576 CSCvh51796	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 exploits that use CPU speculative processing and data cache timing to efficiently leak information, collectively known as Spectre and Meltdown. • CVE-2017-5753 (Spectre/Variant #1) and CVE-2017-5754 (Meltdown) are addressed by applying relevant Operating System patches. • CVE-2017-5715 (Spectre/Variant #2) is addressed by relevant Operating System patches using an interface provided by microcode in the processor.	The fix for CVE-2017-5715 (Spectre/Variant 2) requires updated microcode from Intel. For more information, please see the Cisco Security Advisory at https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180104-cpusidechannel .	2.2(1b)B 2.2(1b)C
CSCvi39280	The System Event Log (SEL) reports "UPI Correctable "Rx / Tx Data Lane 0 is dropped / down"" error messages on UCS B480 M5 and C480 M5 servers. These UPI error messages are reported only on UPI Port 2 for each processor present on the system. The UPI error messages are reported during POST only on 4S configuration with one of the Intel processor models that support only 2 UPI links. The Cisco PIDs for the supported processor models that support only 2 UPI links are UCS-CPU-5120, UCS-CPU-5118, UCS-CPU-5122, and UCS-CPU-5115. On these processor models, only UPI Port 0 and Port 1 are supported by Intel. Because UPI Port 2 is not supported, the BIOS reports that the UPI Port 2 link is down, which is expected. These UPI error messages are benign messages (false errors) reported on unsupported UPI port (Port 2) for the 2UPI processor models. There is no functional impact. These UPI error messages can be disregarded under the conditions described here.	There is no known workaround.	3.2(3a)B

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvi16121	The server reboots unexpectedly and the service profile is re-associated when there is a configuration change for a service profile bound to an updating service profile template with a server pool assigned. This happens when the server assigned to the service profile is not part of the server pool.	• Use the initial service profile template instead of updating the service profile template. • If using the updating template, and the service profile is associated, ensure that the server associated to the service profile is in the template's server pool. • Unbind the service profile from the updating service profile template.	3.2(1d)A
CSCvi13640	After updating blade or rack-mount server firmware through Prepare for Firmware Install, the server firmware is updated, but the status is displayed as Upgrading even after reboot and power cycle for components that do not have firmware updates.	There is no known workaround.	3.2(3a)A
CSCva74263	In Cisco UCS Mini, the QoS buffer does not drain out. As a result, the FI does not transmit any more packets. Further, control protocols such as LACP and CDP also stop.	Reboot the system.	3.1(1e)A
CSCvf88524	Creating and storing kernel dump on any alternate drive (other than C drive) corrupts the OS even if the Challenge-Handshake Authentication Protocol (CHAP) is enabled in the boot policy and in iSCSI SAN.	Use LUN number zero for dump.	3.1(3a)B
CSCvh79589	In normal operation state, the UCS 6332 Series Fabric Interconnects reboots because the bcm_usd process crashes.	There is no known workaround.	3.2(2b)A
CSCvh17760	IOM reboots without creating a core because the DCOS HAP control resets.	There is no known workaround.	3.1(1g)A

Defect ID	Symptom	Workaround	First Bundle Affected

CSCvi03903	ENIC driver installation fails on the German version of Win2K16 server with the following error:
	`This operation was returned because of timeout.`
	`If you know the manufacturer of the device, you can search for driver software on the corresponding website in the support section`
		1. Open **Device Manager**.
		2. From the device list, find the device for which the driver installation failed.
		3. Right-click the device which is unrecognized device or **Unbekanntes Gerät** and select **Uninstall**.
			3.2(2b)B

CSCve53858	The FI QoS queues are stuck, and the traffic is not forwarded after enabling/disabling ports and creating/deleting port channels.	There is no known workaround.	3.2(2b)A
CSCva17452	Packets are dropped at the UP ports of the Cisco UCS 6332-16IUP Fabric Interconnect Series when two no-drop classes (one Ethernet and one FCoE) are configured on the system.	Configure the no-drop Ethernet class as drop class, or move the ports to the non-UP ports.	3.1(1e)A
CSCup85336	FCoE frames are dropped and traffic is interrupted between VIC adapter and storage causing the FCoE IOs to abort. Retries occur when either the Ethernet uplink port is flapped or FCoE uplink is flapped to which the vHBA is not pinned.	Workaround is not required. IOs are aborted and retried and the system recovers automatically.	2.2(2c)A
CSCva37355	In Cisco UCS Mini, after an unsuccessful upgrade from 3.1(1e) to 3.1(1g), all the service profiles and service profile templates are deleted automatically. After a successful upgrade, the service profiles and service profile templates cannot be recovered.	There is no known workaround.	3.1(1e)A
CSCvh60768	VMware VMNIC label changes when a VMNIC in the middle is removed. For example, if the VMNICs range from vmnic0 to vmnic2, and vmnic1 is removed, then after reboot, vmnic2 is renamed as vmnic1.	Manually assign vmNIC number in /etc/vmware/esx.conf file and reboot the server.	3.2(2c)B

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvh69831	In a setup with Cisco UCS B260 and B460 M4 servers with four or more vNICs, after installing ESXi 6.0/6.5, the second half of the vNICs on host port 2 are ordered first in ESXi. Thus, the VMNICs are out of order during initial install.	Manually configure the NIC placement policy so that the second half of the vNICs are ordered first. OR Manually assign the second half of the vNICs to host port 1.	3.1(3b)B
CSCvi12023	Multiple core files are generated when the VICs MTU is changed from 1500 to 9000.	There is no known workaround. The server recovers by itself.	3.2(3a)A
CSCvj01763	While upgrading Cisco UCS Manager to Release 3.2(3a), dynamic vNICs/VFs are not created on servers with VIC 12XX based adapters. VIC 13xx and later adapters are unaffected.	If this issue occurs, downgrade Cisco UCS Infrastructure to a release earlier than Cisco UCS Manager Release 3.2(3a), such as 3.2(2f).	3.2(3a)A Resolved in 3.2(3b)A
CSCvk48744	In UCS blade servers, Serial Over LAN (SOL) and IPMI policies do nor work when configured from Central or Cisco UCS Manager.	There is no known workaround.	3.2(3a)A Resolved in 3.2(3h)
CSCvk36317	After upgrading Cisco UCS Manager from Release 3.1(1l) to 3.2(3b), the existing PVLAN configuration fails because the upstream server in the primary VLAN is unable to reach the VM/Host in the isolated VLAN in the UCS domain.	Configure the affected primary-VLANs as normal VLANs and then back In Cisco UCS Manager GUI, change sharing type to **none** and then back to **primary**.	3.2(3a)A Resolved in 3.2(3h)A
CSCvk40744	When a Cisco UCS C240 M4 Server is associated with a service profile, the service profile does not implement the Core Multiprocessing BIOS token to the server using UCSM BIOS policy. The service profile always configures Core Multiprocessing token value as the default value (**All**) even if a different value is set in the BIOS policy.	While booting the server, press F2 to enter the BIOS settings, and limit the CPU cores.	3.2(3a)A Resolved in 3.2(3h)A
CSCvj74285	Cisco IMC reboots due to Out of memory (OOM) on M5 servers with firmware version 3.1(3a). Cisco IMC is not accessible over a network.	There is no known workaround.	3.2(3a)C Resolved in 3.2(3h)C

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvo60001	A weak MAC was detected on systems running Cisco UCS Manager	N/A	3.2(3a)A Resolved in 3.2(3k)
CSCvm64944	Weak KEX algorithms were detected running in Cisco UCS Manager .	N/A	3.2(3a)A Resolved in 3.2(3k)
CSCvm55258	Cisco M5 Hyperflex server service profile association takes 1 to 2 hours to perform the step "Perform Inventory of Server - PNUOS Inventory".	Check the firmware tab to verify that all drives have Activate Status set as "Ready" before resetting server via KVM/UCSM.	3.2(3a)A Resolved in 3.2(3k)A

Open Caveats for Release 3.2(2f)

The following caveats are open in Release 3.2(2f):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvm81348	Cisco UCS Manager Data Management Engine (DME) crashes due to mismatched adminVcon values passed by Cisco UCS Central for dynamic and static vNICs.	Do not explicitly assign the adminVCon for Dynamic vNICs or their associated Static vNICs.	3.2(2f)A 3.2(3j)A
CSCvm66118	When a PSU with serial number LIT*xxxxxx* is inserted or reseated in a chassis connected to a UCS 6300 Series Fabric Interconnect, it may cause the Fabric Interconnect to report PSU fan faults. However, the PSU LED remains green and the PSU and the fans continue to work.	Do not reseat the PSU unless it is necessary. If reseating or moving the PSU is required, reboot the Fabric Interconnect after the PSU reseating is complete.	3.2(2f)A 3.2(3j)A

Open Caveats for Release 3.2(2d)

The following caveats are open in Release 3.2(2d):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvi57046	The FC-MAC defect causes the following behavior on 6332-16UP fabric interconnects running Cisco UCS Manager Release 3.2(1x) or 3.2(2x): Flapping fc 1/3 will impact fc 1/4 if it is already up Flapping fc 1/4 will impact fc 1/7 if it is already up Flapping fc 1/10 will impact fc 1/11 if it is already up	1/1-2, 1/5-6, 1/8-9, 1/12-16 can be brought up in any order or at any time. When bringing up other ports 1/3-4, 1/7, 1/10-11, follow these guidelines: • Bring-Up 1/3 followed by 1/4 followed by 1/10 followed by 1/7 followed by 1/11 • If any time 1/3 is flapped and if 1/4 is already UP prior to flap of 1/3, 1/4 need to be flapped • If any time 1/4 is flapped and if 1/7 is already UP prior to flap of 1/4, 1/7 need to be flapped So, when 1/3 is flapped you will first need to flap 1/4 followed by flap of 1/7 • If any time 1/10 is flapped and if 1/11 is already UP prior to flap of 1/10, 1/11 need to be flapped	3.2(2d)A Resolved in 3.2(3b)A
CSCvh81553	UCS S3260 M4 servers in an S3260 chassis integrated with Cisco UCS Manager fail discovery after upgrade from Cisco UCS Manager Release 3.1(3c) to 3.2(2d). The discovery process is stuck at PNUOS Ident (57%). Through KVM, it is seen that POST is completing successfully, but PNUOS does not load.	There is no known workaround. Upgrade server firmware to a release in which this issue was resolved.	3.2(2d)C Resolved in 3.2(3a)C
CSCvk51589	Cisco Fabric Interconnect reboots with the following message: `Reset triggered due to HA policy of Reset`	There is no known workaround.	3.2(2d)A Resolved in 3.2(3h)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvm68038	After the tech support logs are downloaded, samdme user sessions do not get cleared from the subordinate FI. This leads to multiple unresponsive sessions, and after the session count on the subordinate FI reaches 64 (maximum allowed), remote access to the FI is lost.	Contact TAC to load the debug plugin on the FI to clear the stale sessions. Generate the Tech-support file from CLI, but download from GUI.	3.2(2d)A Resolved in 3.2(3i)A
CSCvn72558	Cisco M2 blades servers report invalid temperature sensor readings to the IOM, causing the IOM to throw a fault for critical thermal events, and spin up the fans as a safety measure.	None. The temperature readings are invalid.	3.2(2d)A Resolved in 3.2(3k)
CSCvn81327	The Cisco UCS-IOM-2304 IO Module crashes and produces a kernel core dump pointing to `pick_next_task_rt` in certain situations. Traffic forwarding ceases until a watchdog timer triggers a reboot.	N/A	3.2(2d)A Resolved in 3.2(3k)

Open Caveats for Release 3.2(2b)

The following caveats are open in Release 3.2(2b):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvi26150	When using UCSB-PSU-2500ACDV with Grid or N+1 power policy in Cisco UCS Manager Releases 3.2(2b) or 3.2(2d), Cisco UCS Manager reports power redundancy failed due to "mix of high-line and low-line PSU input power sources" The low-line sources are classified when readings from PSU are as follows: `get_ps_input_and_max_power:PSU2: ignoring bad reading, 65535W`	There is no known workaround. After a valid reading is available, the IOM clears this transient condition.	3.2(2b)B Resolved in 3.2(3b)B
CSCvi96785	On UCS 6332-16UP and 6332 fabric interconnects, the file system is corrupted and the **show logging** log or **show logging nvram** log contains a message with the term "EXT3-fs error”.	If this issue occurs, performing a file system check may help. To repair a file system, contact TAC.	3.2(2b)A Resolved in 3.2(3g)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvj91316	When running Cisco UCS Manager 3.2(2b) with Cisco UCS 2304 IOM/FEX, the FEX may corrupt TX frames on the Network Facing port (NIF). This will be reported as input errors on the connected FI ports. The IOM may reboot with CMC logs showing the following error: `Module 1: Runtime diag detected minor event: Forwarding ASIC Buffer failure.`	Reduce the number of NIFs to 2 and ensure that the port channel is configured,	3.2(2b)A Resolved in 3.2(3g)A
CSCvj83780	Under specific low write and long idle time workloads, the following SATA SSDs may show read errors: • UCS-M2-240GB • HX-SD38TBM1K9 • HX-SD38TBE1NK9 • HX-SD960GBM1K9 • HX-SD960GBE1NK9 • HX-M2-240GB In an HX cluster, the drive errors are handled by HyperFlex data platform by putting the drive in a "blacklisted" state. When there are several drive errors the drive will get permanently blacklisted.	Non HyperFlex UCS Servers: Upgrade to Cisco UCS Manager Release 3.2(3e) or later releases. HyperFlex Servers: For HXAF220 M4 and HXAF240 M4 servers with the specific drive PIDs identified: • Contact TAC to perform a rolling upgrade to HXDP version 3.0.1c For All HX M5 servers: • For systems with only HX-M2-240GB, upgrade Cisco UCS Manager to Release 3.2(3e) or later releases. This is the only required step. • For systems with 960G or 3.8TB SED SSDs, refer the field notice.	3.2(2b)B Resolved in 3.2(3e)B

Defect ID	Symptom	Workaround	First Bundle Affected
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 fails. The upgrade remains stuck in the Activating state. Upgrade/Downgrade results in: • Remote Invocation Result : Service Unavailable • Remote Invocation Error Code : 4125 • Remote Invocation Description : BIOS Update Failed: Unable to flash new BIOS Image	Do one of the following: • Upgrade the UCS domain to Cisco UCS Manager Release 2.2.8, perform server firmware updates, then upgrade the UCS domain to Cisco UCS Manager Release 3.x. • Create a custom Host Firmware Package that does not attempt to change the BIOS code. (Either uncheck or utilize BIOS in the exclusions list.)	3.2(2b)A Resolved in 3.2(3b)A

CSCvj03597	Updating the BIOS on UCS B480 M5 blade servers fails with the following status:
	`UCSM FSM status:`
	`Remote Result: End Point Failed`
	`Remote Error Code: ERR UPDATE Failed`
	`Remote Error Description: Flash write failed. Flash on server appears to be bad.`
	`Status: Associate Fail`
	`Previous Status: Associate Fail`
	`Timestamp: <time-stamp>`
	`Progress (%): <%>`
	`Current Task: Waiting for BIOS update to complete(FSM-STAGE:sam:dme:ComputePhysicalAssociate:PollBiosUpdateStatus)`
		There is no known workaround.	3.2(2b)B
			Resolved in 3.2(3b)B

CSCvh76070	UCS B200 M5 servers have connectivity issues with SD cards.	There is no known workaround.	3.2(2b)B Resolved in 3.2(3a)B
CSCvg11168	On large scale setups, the secondary FI (B) crashes continually after the following sequence of events: **1.** Decommission/recommission servers. **2.** Change cluster lead. **3.** Collect UCSM tech-support logs from console: FI:A	There is no known workaround.	3.2(2b)A Resolved in 3.2(3a)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvh32617	UCS B480 M5 blade servers that are fully loaded with 48*128G DIMMs and UCS-CPU-8176M fail discovery. The discovery process remains at the Pnuos Ident stage.	If this issue occurs, upgrade Cisco UCS Manager to Release 3.2(2f) or later releases.	3.2(2b)A Resolved in 3.2(2f)A
CSCvi06930	Discovery of UCSC-C480-M5 through Cisco UCS Manager fails when more than 10 NVMe drives are populated.	If this issue occurs, reduce the maximum number of NVMe drives to 9.	3.2(2b)A Resolved in 3.2(2f)A
CSCvg06395	While configuring RAID60 virtual drives on a Cisco UCS S3260 setup, Cisco UCS Manager displays the following configuration failure error even through enough space is left in existing disk groups: `Insufficient disks for the specified RAID level`	If this issue occurs, use the Avago or LSI utility to create the virtual drives on existing disk groups.	3.2(2b)C Resolved in 3.2(3a)C
CSCvf51664 CSCvg08158	Multicast data traffic received on the FI uplink with Secondary VLAN gets dropped because the Designated Receiver (DR) for the VLAN is a different uplink interface. This happens when: • The FI is in EHM mode with more than two uplink border ports, and PVLAN is Enabled. • The Primary and Secondary VLANs are pinned to different uplink DR ports because of a specific trigger (Border Port where Primary/Secondary VLAN are initially pinned (DR) flaps) • Traffic for the Secondary VLAN gets received on the uplink acting as DR for the Primary VLAN.	Restrict the number of border uplinks to two or less than two.	3.2(2b)A Resolved in 3.2(3a)A
CSCvg78583	Cisco UCS Manager may not display the local disk catalog details on the C240 M5.	There is no known workaround.	3.2(2b)C Resolved in 3.2(2d)C
CSCvh00935	Cisco IMC may incorrectly report a hard disk drive temperature as hot.	There is no known workaround.	3.2(2b)A Resolved in 3.2(2d)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvg93195	An IOM thermal core on a 3GFI setup may occur.	There is no known workaround.	3.2(2b)B Resolved in3.2(2d)B
CSCvh02465	Cisco UCS Manager may not display the physical location of the NVME drive.	There is no known workaround.	3.2(2b)A Resolved in3.2(2d)A
CSCvf70114	After enabling the usnic policy in a service profile, the Linux virtual machine may not boot due to a PCI-E error.	To avoid this, do not enable the usnic from a service profile or move to a different server.	3.2(2b)C
CSCvg50989	ESXi 6.5 installation failure on SD cards is observed on UCS M5 servers with error messages similar to one of the following: • `vmkfstools failed with message: bcreate fs` • `partedUtil failed with message: b'Error: Cound not stat device` • `partedUtil failed with message: b'Unable to get device` In HX environments, installation fails with the following deployment error: `Updating Cluster Progress Step:,Step(Configuring Hypervisor,Failed, None,Some(EntityRef(failed with ' [StatelessError]`	There is no known workaround.	3.2(2b)B Resolved in 3.2(2c)B
CSCvg50400	While upgrading firmware when there is heavy I2C traffic,the storage controller firmware hits exceptions resulting in firmware download failures.	If this issue occurs, retry the flash upgrade operation until it succeeds	3.2(2b)C Resolved in 3.2(2c)C
CSCvg52570	When using VIC Firmware version 4.2(2a) with Cisco UCS Manager Release 3.2(2b) and UCS C-Series Software Release 3.1(2b), FCoE performance may drop with workloads involving IO sizes less than 32K.	Use VIC Firmware version 4.2(2b) or later versions.	3.2(2b)B Resolved in 3.2(2c)B

Defect ID	Symptom	Workaround	First Bundle Affected

CSCvj08442	After adding the Secondary Fabric Interconnect to the cluster, the Fabric Interconnect fails to configure FC ports in FC switching mode. In the Cisco UCS Manager GUI, the Fabric Interconnect appears incorrectly as in FC switching mode. However, using the following command, the Fabric Interconnect appears to be in 'end-host' mode.
	`FI-B(nxos)# show platform fwm info lif all`
	`dump lif info: if_index 0x0 dump_all 1 verbose 0`
	`fc1/1: state 0x2 if_ord 0 if 'pif fc1/1'`
	`fc1/1: mode 'end-host' pinned-if 'none' if-type 'none' sif_nf_exporter=NO ' <<<<< mode 'end-host'`
	This issue occurs when all the following conditions are met:
	• Fabric Interconnect is configured in Ethernet switching mode and/or FC switching mode
	• The UCS Infrastructure bundle running is Cisco UCS Manager Release 3.2(3a)
	• The Secondary Fabric Interconnect is replaced in the HA cluster, or is added to the HA cluster, or the Primary Fabric Interconnect was in standalone mode (with Ethernet and/or FC switching mode configured) and the new cluster is formed with the secondary Fabric Interconnect joining the cluster.
		There is no software workaround to avoid this issue if the conditions mentioned occur.
		To recover after the issue occurs, downgrade Cisco UCS Manager and/or the Infrastructure bundle (A) to a release earlier than Release 3.2(3a)A. After all configurations are applied to the secondary FI, upgrade the infra(A) bundle back to 3.2(3a)A.
		To recover with TAC help, contact TAC.
		Other recovery options:
		• After the HA cluster is formed with Release 3.2(3a), change the mode to end-host mode (if the earlier configured mode was switching mode). The Fabric Interconnects will get reloaded one-by-one to get end-host mode applied.
		• Reconfigure from end-host mode to switching mode (in HA cluster mode). The Fabric Interconnects will get reloaded one-by-one to get switching mode applied.
			3.2(2b)A
			Resolved in 3.2(3d)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvh75430	On a Cisco UCS Manager 3.2(2) system configured with **Allowed SSL protocols** set to **Only TLS 1.2**, the Cisco UCS KVM Direct login page allows TLS version 1.0 on Out of Band (OOB) addresses.	If Direct KVM access is not needed for UCS blade servers or rack servers integrated with Cisco UCS Manager, disable the **CIMC Web Service** communication service on Cisco UCS Manager.	3.2(2b)A Resolved in 3.2(3d)A
CSCvi80895	After upgrading to Release 3.2(2c), TACAC users are unable to create full local backup of Cisco UCS Manager.	Backup Cisco UCS Manager using local admin user account.	3.2(2b)A Resolved in 3.2(3h)A
CSCvj45253	In a setup with Cisco UCS B200 M5 Server or Cisco UCS B480 M5 Server, sometimes the FlexFlash Controller is not detected. This is caused due to command timeout.	Upgrade CIMC to 4.1(27a) found in UCS 4.0(1a)B bundle to restore FlexFlash connectivity. After FlexFlash connectivity is restored downgrade CIMC back to original version.	3.2(2b)A Resolved in 3.2(3h)A
CSCvh70412	Cisco UCS Manager displays blade server discovery failure messages after port flaps on the link between IOM and FI.	No known workaround.	3.2(2b)A Resolved in 3.2(3j)A
CSCvi26526	B200 M5 Blade Servers, as well as Hyperflex, displayed a false warning of low memory when the kernel actually has free memory, but has allocated the memory in reusable system cache that is reclaimed on demand.	This condition can be ignored. It is a false warning of low memory when the kernel actually has free memory.	3.2(2b)B Resolved in 3.2(3k)B
CSCvh87378	Servers in community VLAN are not able to communicate with the primary VLAN after upgrade to UCS Manager version 3.1(3) or above.	Move the promiscuous port (primary VLAN) outside the UCS.	3.2(2b) Resolved in 3.2(3l)A

Open Caveats for Release 3.2(1d)

The following caveats are open in Release 3.2(1d):

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 3.2(3g)B, 3.2(3g)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 3.2(3g)B, 3.2(3g)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 3.2(3g)B, 3.2(3g)C

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvm03339	Cisco UCS B-Series M5 servers, C-Series M5 servers, and HyperFlex M5 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 CSCvm03339 is resolved in 3.2(3g)B, 3.2(3g)C
CSCvj59299 CSCvj59301	Cisco UCS B-Series and C-Series M2 servers are based on Intel® Xeon® EP 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 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180521-cpusidechannel	3.2(1d)B, 3.2(1d)C 3.1(1e)B, 3.1(1e)C 2.2(1b)B, 2.2(1b)C CSCvj59299 is resolved in 3.2(3g)B, 3.2(3g)C

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvj54880	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 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 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180521-cpusidechannel	3.2(1d)B, 3.2(1d)C 3.1(1e)B, 3.1(1e)C 2.2(1b)B, 2.2(1b)C 3.0(1c)B, 3.0(1c)C Resolved in 3.2(3g)B, 3.2(3g)C
CSCvj54847 CSCvj54187	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 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 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180521-cpusidechannel	3.2(1d)B, 3.2(1d)C 3.1(1e)B, 3.1(1e)C 2.2(1b)B, 2.2(1b)C 3.0(1c)B, 3.0(1c)C - Only for M4 EP Resolved in 3.2(3e)B, 3.2(3e)C

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvj59266	Cisco UCS and Hyperflex M5 servers are based on Intel® Skylake 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 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180521-cpusidechannel	3.2(1d)B, 3.2(1d)C Resolved in 3.2(3g)B, 3.2(3g)C

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

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvh22485	In a VMFEX setup with PVLAN host configurations on the Veths, after vMotion or VM migration, VMs are unable to receive broadcast or multicast packets, including ARP packets. This issue does not occur if the VMs are powered off before migration.	Do not perform vMotion or VM migration. If needed, power-off the VM before migration and then power-on again. If this issue occurs, power cycle the VM after vMotion.	3.2(1d)A Resolved in 3.2(3a)A
CSCvh55047	In a system with UCS M5 servers and UEFI SAN boot policy, bladeAG cores may be generated. This causes blade servers to go into shallow discovery. Any new service profile association also fails.	If this issue occurs, recomission and decomission the affected blade servers.	3.2(1d)A Resolved in 3.2(2f)A and 3.2(3a)A
CSCvf15927	The Matrox display driver shows error code 43 and provides a reduced display resolution on B260 and B460 M4 blade servers with Windows Server 2016.	There is no known workaround for this issue.	3.2(1d)B Resolved in 3.2(3a)B
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
CSCvg92817	After upgrading to Cisco UCS Manager Release 3.2, and with the power policy set to Grid Power, Call Home alerts are generated occasionally, indicating redundancy power lost although the right number of power supplies are present and active to satisfy the Grid Power policy.	There is no known workaround for this issue.	3.2(1d)B Resolved in 3.2(3a)B
CSCve34690	FlexFlash SD storage may fail with a missing fault.	Reboot the host to boot off the 2nd SD Card if the mirrored config was present previously. Configure a call home level of "informational" to receive equipment missing faults.	3.1(2b)A Resolved in 3.2(1d)A
CSCvg62341	OS driver information may not be displayed after upgrading or downgrading Cisco IMC.	There is no known workaround.	3.1(2b)C Resolved in 3.2(2d)C
CSCvg74318	Cisco UCS Manager may generate a fault for a fan module that is not installed on the C240 M5.	There is no known workaround.	3.1(2b)C Resolved in 3.2(2d)C

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvf89931	Broadcom SAS IT controller firmware fails to initialize the I2C interface correctly, resulting in the BMC being unable to communicate with the controller through the I2C bus.	Resetting or reassociation usually brings the link back up. Sometimes, multiple reassociation attempts may be required to bring the link back up.	3.2(1d)C Resolved in 3.2(2c)C
CSCve47615	The **TPM Clear** operation initiated through Cisco UCS Manager does not clear the TPM module.	Go to BIOS Setup (press the F2 key during POST), and clear the TPM manually. If TPM is not enabled, first enable TPM through BIOS Setup, reboot the server, and then clear TPM.	3.2(1d)B Resolved in 3.2(2b)B
CSCve49653	When TXT is enabled from Cisco UCS Manager BIOS policy, the system intermittently fails to power on.	There is no known workaround.	3.2(1d)B Resolved in 3.2(2b)B
CSCve88355	For UCS M5 servers, after upgrading or activating the BIOS, the core count set in the tokens and the actual applied count differs.	Set the token again using service profiles.	3.2(1d)B
CSCvf23628	UCS B200 M5 blade servers using SATA SSDs may fail VMware VSAN certification in an All Flash configuration. UCS M4 blade servers running on Cisco UCS Manager Release 3.2(1d) driver ISO fail VMware VSAN certification.	For UCS B200 M5 blade servers, use either SAS or NVME drives instead of SATA SSDs during VSAN certification with All Flash configuration. For UCS M4 blade servers, use the Cisco UCS Manager Release 3.1(3) driver ISO, and do not upgrade to a Release 3.2(1d) driver ISO.	3.2(1d)B Resolved in 3.2(2b)B
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

Defect ID	Symptom	Workaround	First Bundle Affected
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
CSCvf84205	When IGMP Snooping is enabled on the FI, the FI reboots with IGMP hap reset.	When this issue occurs, disable IGMP Snooping on the FI and uplink switch	2.2(8f)A
CSCvf33668	While upgrading the infrastructure firmware using AutoInstall 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)
CSCvh07445	Under heavy traffic, Cisco B200 M5 blade servers fail discovery and show the message: DME Logs: Remote-Invocation-Error: CimcVMedia Error: Error retrieving vmedia attributes list-MC Error(-6): Connection is closing	None	3.2(1d) Resolved in 3.2(3k)B

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.

vNIC and vHBA Provisioning on Cisco UCS Manager-Integrated C-Series Adapters

Beginning with Cisco UCS Manager Release 3.2(2b), Cisco UCS Manager supports vNIC and vHBA provisioning on specific Cisco UCS Manager-integrated C-Series adapters. The complete list of these adapters is available in the *Cisco UCS C-Series Server Integration with Cisco UCS Manager 3.2* guide.

Infrastructure and Cisco UCS Manager Version Mismatch

In Cisco UCS Manager Release 3.2(3d), the following versions are mismatched:

- The Cisco UCS Manager login displays the version as 3.2(3c).

- Under **Equipment** > **Firmware Management** > **Installed Firmware**, **Package Version** appears as 3.2(3d)A for FIs and Cisco UCS Manager, but **Running Version** appears as 3.2(3b).

OEM Bit Marker for Azure Stack Not Supported

CSCvj03972—Beginning with Cisco UCS Manager Release 3.2(3b), Cisco UCS Manager no longer supports the OEM bit marker for Azure Stack.

Mode Change Supported for P6 GPUs

While using P6 GPUs with UCS B200 M5 servers, the GPUs now change successfully into graphics mode through the Cisco UCS Manager graphic mode policy, and service profile association occurs without any configuration errors.

In releases earlier than Cisco UCS Manager Release 3.2(3), associating a service profile with a graphics card policy (graphics mode) to B200 M5 servers with P6 GPUs would fail with the following configuration error on both servers:

```
Mode change is not supported for this graphics card model
```

Chassis-Specific Power Details

In releases earlier than Cisco UCS Manager Release 3.2(3), the Cisco UCS Manager GUI displayed only **Power Group** details under the **Equipment** > **Chassis** > **General** tab. This tab now displays chassis-specific power details.

MD5 SNMPv3 User Authentication Not Supported in FIPS Mode

Cisco UCS Manager Release 3.2(3) and later releases do not support MD5 authentication if SNMPv3 is in Federal Information Processing Standards (FIPS) mode. Hence, any existing or newly created SNMPv3 users with MD5 authentication will not be deployed with these releases and the following fault message will appear:

```
Major     F1036    2018-02-01T14:36:32.995     99095 SNMP User testuser can't be
deployed. Error: MD5 auth is not supported
```

To deploy such a user, modify the authentication type to **SHA**.

SNMPv3 User Without AES Encryption Not Supported

Cisco UCS Manager Release 3.2(3) and later releases do not support SNMPv3 users without AES encryption. Hence, any existing or newly created SNMPv3 users without AES encryption will not be deployed with these releases, and the following fault message will appear:

```
Major     F1036    2018-02-01T14:36:32.995     99095 SNMP User testuser can't be
deployed. Error: AES is not enabled
```

To deploy such a user, enable **AES-128** encryption.

Fabric Interconnect Replacement

To replace an FI in a cluster on Cisco UCS Manager Release 3.2(3) with an FI on a release earlier than Cisco UCS Manager Release 3.2(3), FIPS mode must be disabled (**disable fips-mode**) on the existing FI before adding the replacement FI to the cluster. After the cluster is formed, as part of the Cisco UCS Manager boot up, FIPS mode is automatically enabled.

Pasting Enabled for Login Password Field

CSCvf08548—Starting with Cisco UCS Manager Release 3.2(2b), pasting to the **Password** field of the Cisco UCS Manager login page has been enabled.

M5 Server BIOS Defaults

Cisco UCS Manager Release 3.2(1) and later releases do not use default BIOS policies for UCS M5 servers. UCS M5 servers ship with default BIOS settings, which can be changed by applying a BIOS policy with the changed settings.

For the complete list of M5 BIOS tokens, defaults, and values for each 3.2(x) release, refer to the *Cisco UCS M5 Server BIOS Tokens Guide* available at the following URL: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/Reference-Docs/Server-BIOS-Tokens/3-2/b_UCS_BIOS_Tokens.html

Minimum UCS Chassis Fan Speed Increased

When running Cisco UCS Manager Release 3.2(1) and later releases with UCS M5 blade servers, the minimum chassis fan speed is now 5100 rpm instead of 3300 rpm.

Audit Log

CSCvd66733—In Cisco UCS Manager Release 3.2(1d) and later releases, AAA authentication failure information is reported as syslog messages so that data can be captured at a remote server or in the syslog file on the FI.

Sensor Reduction and Integration for UCS M5 Servers

CSCvd51613—Starting with Cisco UCS Manager Release 3.2(1d), the processor current sensor values for UCS M5 servers have been deprecated. The **Statistics** tab for an M5 server will now display each processor's **Input Current** as **N/A**.

Incorrect Disk Numbering for Disks Managed by PSATA onboard RAID Controller on UCS C220-M5SX

CSCve92554—In Cisco UCS Manager Release 3.2(1d) and later releases, disks managed by the PSATA onboard RAID controller may be incorrectly numbered on UCS C220-M5SX servers.

The front disks, which are managed by the PSATA onboard controller on a UCS C220-M5SX server, may be numbered incorrectly in the Cisco UCS Manager GUI and CLI. Disk numbering on a UCS C220-M5SX server is from 1 to 10, and the PSATA controller can only manage disks that are in slots 1 to 4 and slots 6 to 9. Disks in slot 5 and 10 are not managed by the PSATA controller.

Although a disk in slot 5 is not managed by PSATA, Cisco UCS Manager inventory shows a disk in slot 5 as present. This is due to a mismatch in disk slot mapping. Disks in slot 6,7,8, and 9 are shown as 5,6,7, and 8 respectively in Cisco UCS Manager GUI and CLI.

Disk and FlexFlash Scrub

CSCve53092—For a server associated with a service profile, disk scrub and FlexFlash scrub occur during disassociation, based on the scrub policy used in the service profile. For an un-associated server, disk scrub and FlexFlash scrub occur during the server discovery process, based on the default scrub policy.

TXT Mode

CSCve49653—In Cisco UCS Manager Release 3.2(1d), TXT mode is not supported.

Cisco UCS Manager Release 3.2(2b) and later releases support TXT mode.

QoS Traffic Paused

CSCvh06851—In a setup with blade servers and the 2200 Series IOM/FEX, the QoS traffic is paused due to mix up of Drop and No-Drop QoS class traffic. The IOM sends the incomplete value of the user-configured PFC priority map, due to which all QoS classes are treated as No-Drop. Hence, on the Adaptor data path, the No-Drop QoS class and the Drop QoS class are configured in the same Egress Queue.

ENIC 2.3.0.30 Driver Version Failure

CSCva84733—ENIC driver version 2.3.0.30 does not work with xs6.5 and xs7.0 in bridge mode. In this setup, the system fails to get an IP address.

Workaround

1. Remove eth0.0 from xenbr0.
2. Add eth0 to xenbr0.
3. From the XS menu, renew the DHCP lease.

   Or, you can also renew the DHCP manually from the console.