

Known issues

The open and resolved bugs for a release are accessible through the Cisco Bug Search Tool.

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.

- Known issues in Cisco UCS B-Series M5 6.0(1.260031) Server Firmware Release — None, on page 2
- Known issues in Cisco UCS B-Series M5 6.0(1.260012) Server Firmware Release — None, on page 2
- Known issues in Cisco UCS X-Series M8, M7, M6 6.0(2.260040), XE-Series M8 6.0(2.260042), C-Series M8, M7, M6 6.0(2.260044), and B-Series M6 6.0(2.260040) Server Firmware Release, on page 2
- Known issues in Cisco UCS XE-Series M8 Server Firmware Release, 6.0(1.260001) — None, on page 4
- Known issues in Cisco UCS C-Series M8 6.0(1.250194) Server Firmware Release — None, on page 4
- Known issues in Cisco UCS X-Series M8 6.0(1.252114), M7, M6 6.0(1.250179), B-Series M6, M5 6.0(1.250169), and C-Series M8, M7, M6 6.0(1.250192) Server Firmware Release — None, on page 4
- Known issues in Cisco UCS XE-Series M8 Server Firmware Release, 6.0(1.251030), on page 4
- Known issues in Cisco UCS X-Series M8, M7, M6 6.0(1.250162), B-Series M6, M5 6.0(1.250157), and C-Series M8, M7, M6 6.0(1.250174) Server Firmware Release — None, on page 5
- Known issues in Cisco UCS X-Series M8, M7, M6 6.0(1.250122), B-Series M6, M5 6.0(1.250127), and C-Series M8, M7, M6 6.0(1.250131) Server Firmware Release — None, on page 5
- Known issues in Cisco UCS C-Series M8, M7, and M6 6.0(1.250127) Server Firmware Release, on page 5

Known issues in Cisco UCS B-Series M5 6.0(1.260031) Server Firmware Release — None

Known issues in Cisco UCS B-Series M5 6.0(1.260012) Server Firmware Release — None

Known issues in Cisco UCS X-Series M8, M7, M6 6.0(2.260040), XE-Series M8 6.0(2.260042), C-Series M8, M7, M6 6.0(2.260044), and B-Series M6 6.0(2.260040) Server Firmware Release

This section provides a brief description of the known issues.

Defect ID	Description	Workaround	First Version Affected

CSCwr72707	On fully populated Cisco UCS C220 M8, C240 M8, or UCSXE130C M8 nodes with more than two Kioxia E3.S CD8P 1.9 T NVMe drives, random workload performance drops significantly during concurrent tests. Specifically, 4K random read performance may drop from a rated 1,600kIOPS per drive to approximately 680k Input/Output Operations Per Second (IOPS) per drive during concurrent operations. Single drive tests meet expected performance, indicating the issue only occurs with multi-drive setups	To resolve this performance bottleneck, apply the following Intel-recommended kernel tuning parameters in the Red Hat Enterprise Linux (RHEL) boot configuration:
		• For single-drive configurations: Add the following to the RHEL kernel command line:
		`intel_pstate=disable`
		`pcie_aspm.policy=performance`
		`pci=pcie_bus_safe`
		• For multi-drive (fully populated) configurations: Add the following to the RHEL kernel command line:
		`intel_pstate=disable`
		`pcie_aspm.policy=performance`
		`pci=pcie_bus_safe`
		`nvme.poll_queues=32`
		`intel_iommu=on`
			X-series: 6.0(2.260040)
			XE-series: 6.0(2.260042)
			C-series: 6.0(2.260044)
			B-series: 6.0(2.260040)

Known issues in Cisco UCS XE-Series M8 Server Firmware Release, 6.0(1.260001) — None

Known issues in Cisco UCS C-Series M8 6.0(1.250194) Server Firmware Release — None

Known issues in Cisco UCS X-Series M8 6.0(1.252114), M7, M6 6.0(1.250179), B-Series M6, M5 6.0(1.250169), and C-Series M8, M7, M6 6.0(1.250192) Server Firmware Release — None

Known issues in Cisco UCS XE-Series M8 Server Firmware Release, 6.0(1.251030)

This section provides a brief description of the known issues.

Defect ID	Description	Workaround	First Version Affected
CSCws25068	When installing Ubuntu 24.04.3 with kernel version 6.8.0-71 on the Unified Edge server, the integrated network card (ICE driver) is not detected, preventing network configuration and connectivity. This issue occurs because kernel 6.8.0-71 lacks ICE driver support for the NIC on this platform.	1. Download the GA ISO from the Ubuntu Noble Release Page and install it using a bootable USB or virtual media 2. Download the required 6.8.0-80 kernel packages (`.deb` files) from the Ubuntu Security Pool. 3. Place all `.deb` files (`linux-image`, `linux-headers`, `linux-modules`, `linux-modules-extra`, `linux-tools`) in a folder and create an ISO using a tool like genisoimage or mkisofs. 4. Mount the ISO on the server after installing Ubuntu. 5. Install the kernel packages using `dpkg -i *.deb`. 6. Reboot the server and verify the kernel version is 6.8.0-80. The integrated network card will now be detected and available for configuration.	6.0(1.251030)

Known issues in Cisco UCS X-Series M8, M7, M6 6.0(1.250162), B-Series M6, M5 6.0(1.250157), and C-Series M8, M7, M6 6.0(1.250174) Server Firmware Release — None

Known issues in Cisco UCS X-Series M8, M7, M6 6.0(1.250122), B-Series M6, M5 6.0(1.250127), and C-Series M8, M7, M6 6.0(1.250131) Server Firmware Release — None

Known issues in Cisco UCS C-Series M8, M7, and M6 6.0(1.250127) Server Firmware Release

This section provides a brief description of the known issues.

Defect ID	Description	Workaround	First Version Affected
CSCwn95239	On Cisco UCS C-Series servers, the server may fail to power on due to BIOS corruption. The following message is displayed: "Power on failure asserted [Power on Fail, Server failed to power-on]." This issue can occur in the following scenarios, especially when BIOS update operations are disrupted: • Interrupting a BIOS flash or update (for example, forcing a power cycle during the update). • Initiating a CMOS clear operation during a BIOS update. • Restoring factory defaults during a BIOS update. • Rebooting Cisco IMC during a BIOS update. • Performing other unexpected operations that disrupt the BIOS update process.	Do one of these: • Reboot of CIMC. In-turn, recovery mechanism will start that is bios activation. • Activate of bacup BIOS. • Update and activate BIOS.	4.3(6.250039)

Defect ID	Description	Workaround	First Version Affected
CSCwo68248	On Cisco UCS C220 M7 and C240 M7 servers running HUU 4.3(3.240xxx) level firmware with 2 PCIe VICs and 1 MLOM VIC, upgrading the server firmware to HUU 4.3(4.xxxxxx), 4.3(5.xxxxxx), 4.3(6.xxxxx), or later using the Redfish API interface may cause the UCSUpdate task to falsely report an update failure for the PCIe VIC (riser1) through which CiscoCard mode is configured. However, the firmware is actually updated and activated successfully in the background. **Note** In the mentioned HUU version numbers, "xxxx" represents all versions available within the series.	There is no workaround. Ignore the false failure update.	4.3(3.240043)