Mitigate Microsoft Secure Boot Certificate Expiration

Contents

Introduction

Background Information

Problem

- What Certificates Are Expiring?
- Why Is This a Problem for Cisco UCS Servers?
- What Happens If No Action Is Taken?

Solution

- Apply Cisco UCS Firmware Updates
- Action Steps
- Intersight Managed Mode (IMM) - Servers
  - Blade Servers (B and X - Series)
  - Rack Servers (C-Series) integrated in insightManaged Mode (IMC)
- Standalone Rack Servers (C-Series) - Host Upgrade Utility (HUU)
- UCS Manager (UCSM) - Managed Servers

Introduction

This document describes how to mitigate the upcoming expiration of Secure Boot Certificates as it pertains to Cisco UCS environments.

Background Information

Secure Boot is a foundational security feature built into the Unified Extensible Firmware Interface (UEFI) of modern servers and PCs. It establishes a chain of trust during the boot process by ensuring that only digitally signed and verified software bootloaders, operating system kernels, and UEFI drivers are allowed to execute. This mechanism protects systems against bootkits, rootkits, and other low-level malware threats.

At the heart of Secure Boot lies a set of cryptographic certificates issued by Microsoft. These certificates are embedded in the UEFI firmware of virtually every server and PC shipped in the last decade, including Cisco UCS (Unified Computing System) servers. They serve as the trust anchors that validate whether a piece of boot-time software is legitimate.

Microsoft has now disclosed that critical Secure Boot certificates expire starting on June 2026. This expiration affects the entire hardware ecosystem, and Cisco has acknowledged the impact on its UCS server portfolio under Cisco bug ID CSCwr45526.

Problem

What Certificates Are Expiring?

The three certificates at the center of this issue are:

Certificate	Role	Expiration Date
Microsoft Windows Production PCA 2011	Signs and validates Microsoft Windows bootloaders	June 27, 2026
Microsoft UEFI CA 2011	Signs and validates third-party UEFI drivers, option ROMs, and non-Windows bootloaders	June 27, 2026
Microsoft Corporation KEK CA 2011	Signs updates to DB and DBX.	June 24, 2026

These certificates are stored in the UEFI firmware Secure Boot key stores:

- db (Signature Database) — Contains trusted certificates used to verify boot-time binaries.
- KEK (Key Exchange Key) — Authorizes updates to the Signature Database.
- PK (Platform Key) — The root of trust, typically owned by the OEM (for example, Cisco).

Why Is This a Problem for Cisco UCS Servers?

Cisco UCS servers— B-Series (Blade), C-Series (Rack), and X-Series (Modular) platforms ship with Microsoft 2011 Secure Boot certificates pre-loaded in their UEFI BIOS firmware. When Secure Boot is enabled, the BIOS uses these certificates at every boot cycle to validate:

- The Operating System bootloader, which is signed by the Windows Production PCA 2011.
- Third-party UEFI components, such as:
    - Storage controller (RAID) UEFI drivers
    - Network adapter PXE boot ROMs
    - Other PCIe device firmware loaded during POST

These components are typically signed by the Microsoft UEFI CA 2011.

What Happens If No Action Is Taken?

- Existing operating systems, drivers, and option ROMs continue to function normally, as they were signed with the currently trusted certificates and do not depend on the new certificate authority. Consequently, affected servers continue to boot without interruption. The expiration affects only

future binaries signed with the new certificates, it does not retroactively invalidate previously signed and already-trusted components.
- The point at which files are re-signed with the new certificates is determined by the vendor responsible for each component, not by a single coordinated event. This applies equally to UCS-based appliances, where the timeline is governed by the respective vendors and signing authorities responsible for those images.
- This is not a Windows-specific concern. Any operating system or firmware component that relies on Secure Boot and adopts the new signing certificates are subject to the same transition requirements over time. For this reason, coordination with the responsible appliance vendors is essential. The guidance that each vendor published and advisories is to be tracked directly, rather than assuming that an underlying UCS firmware update alone is sufficient since the appliance operating system image signing is controlled separately from the platform firmware.

This table summarizes the expected boot behavior based on the CIMC certificate state and whether Secure Boot is enabled. It illustrates where remediation (updating CIMC to the new certificate) is required to preserve the ability to boot future signed files:

CIMC Certificate State	Secure Boot Enabled	Secure Boot Enabled –	Secure Boot Disabled	Secure Boot Disabled
	Current Files	Future Files	Current Files	Future Files
Old CIMC (old cert)	O	X	O	O
New CIMC (new cert)	O	O	O	O

Legend: O = Boots successfully · X = Boot failure / files not trusted

Cisco has formally tracked this issue under Cisco bug ID CSCwr45526.

This defect acknowledges that:

- UCS server firmware contains the expiring Microsoft 2011 Secure Boot certificates.
- A firmware update is required to introduce the replacement certificates (Microsoft 2023 certificates) into the UEFI key stores.

Note:The Secure Boot certificate issue does not occur if the UCS server runs in Legacy Boot mode. Similarly, UEFI mode with Secure Boot disabled remains unaffected.

Solution

Apply Cisco UCS Firmware Updates

Updated firmware for affected UCS platforms that includes the new Microsoft Secure Boot certificates:

New Certificate	Replaces
Microsoft Windows UEFI CA 2023	Microsoft Windows Production PCA 2011
Microsoft UEFI CA 2023	Microsoft UEFI CA 2011
Microsoft Corporation KEK 2K CA 2023	Microsoft Corporation KEK CA 2011

Action Steps

- Monitor Cisco bug ID CSCwr45526 on the Cisco Bug Search Tool for fixed firmware versions and release timelines.
- Download and deploy the updated firmware when available for your specific UCS platform (B-Series, C-Series, X-Series).
- Use Cisco management tools for firmware Upgrade:
  - Cisco Intersight — For cloud-managed environments, use Intersight firmware management policies to orchestrate updates at scale.
  - Cisco UCS Manager (UCSM) — For domain-managed B-Series and C-Series servers.
  - Cisco IMC (Integrated Management Controller) — For standalone C-Series rack servers.

The next tables contain the minimum firmware version that includes the fix with the updated certificates, versions higher also contain fix:

Intersight Managed Mode (IMM) - Servers

Blade Servers (B and X - Series)

Server Model	Firmware Version(s)
UCSB-B200-M5	5.4.0.260011
UCSB-B480-M5	5.4.0.260011
UCSB-B200-M6	5.4.0.260011, 6.0.2.260040
UCSX-210C-M6	5.4.0.260009, 6.0.2.260040
UCSX-210C-M7	5.4.0.260010, 6.0.2.260040
UCSX-410C-M7	5.4.0.260010, 6.0.2.260040
UCSX-210C-M8	5.4.0.260010, 6.0.2.260040
UCSX-215C-M8	5.4.0.260010, 6.0.2.260040
UCSX-410C-M8	6.0.2.260040

Rack Servers (C-Series) integrated in insight Managed Mode (IMC)

IMC Firmware Version
IMC-6.0.2.260044
IMC-6.0.2.260043
IMC-6.0.2.260042
IMC-6.0.2.260040
IMC-6.0.2.260026
IMC-5.4.0.260011
IMC-5.4.0.260010
IMC-5.4.0.260009
IMC-4.3.6.260017
IMC-4.3.2.260007

Standalone Rack Servers (C-Series) - Host Upgrade Utility (HUU)

Server Model	Firmware Version(s)
UCSC-C125	4.3.2.260007
UCSC-C220-M5	4.3.2.260007
UCSC-C220-M6	4.3.6.260017, 6.0.2.260044
UCSC-C220-M7	4.3.6.260017, 6.0.2.260044
UCSC-C220-M8	4.3.6.260017, 6.0.2.260044
UCSC-C225-M6	4.3.6.260017, 6.0.2.260044
UCSC-C225-M8	4.3.6.260017, 6.0.2.260044
UCSC-C240-M5	4.3.2.260007
UCSC-C240-M6	4.3.6.260017, 6.0.2.260044
UCSC-C240-M7	4.3.6.260017, 6.0.2.260044
UCSC-C240-M8	4.3.6.260017, 6.0.2.260044
UCSC-C245-M6	4.3.6.260017, 6.0.2.260044
UCSC-C245-M8	4.3.6.260017, 6.0.2.260044
UCSC-C480-M5	4.3.2.260007
UCS-S3260-M5	4.3.6.260017
UCSXE-130C-M8	6.0.2.260042

UCS Manager (UCSM) - Managed Servers

UCSM Firmware Version
4.3(6f)
6.0(2b)

Additional configuration are sometimes required to resolve the UEFI certificate expiration issue, based on the operating system on the UCS servers. Cisco recommends to contact to the respective OS vendor for guidance on the specific remediation steps.



Note: Firmware updates on UCS servers alone do not always fully resolve the issue. OS-level certificate updates can be also necessary to ensure continued Secure Boot functionality beyond the 2026 UEFI certificate expiration date.
