Mitigate Microsoft Secure Boot Certificate Expiration

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 two critical Secure Boot certificates — the **Microsoft Windows Production PCA 2011** and the **Microsoft UEFI CA 2011** — are set to **expire on October 19, 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 two certificates at the center of this issue are:

Certificate	Role	Expiration Date
Microsoft Windows Production PCA 2011	Signs and validates Microsoft Windows bootloaders	**October 19, 2026**
Microsoft UEFI CA 2011	Signs and validates third-party UEFI drivers, option ROMs, and non-Windows bootloaders	**October 19, 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 — including the **B-Series (Blade)**, **C-Series (Rack)**, and **X-Series (Modular)** platforms — ship with these Microsoft 2011 certificates pre-loaded in their UEFI BIOS firmware. When Secure Boot is enabled, the BIOS uses these certificates at every boot cycle to validate:

1. **The Windows Server bootloader** (for example, `bootmgfw.efi`) — signed by the Windows Production PCA 2011.
2. **Third-party UEFI components** such as:
   - Cisco VIC (Virtual Interface Card) option ROMs
   - Storage controller (RAID) UEFI drivers
   - Network adapter PXE boot ROMs
   - Any other PCIe device firmware loaded during POST

   These are typically signed by the Microsoft UEFI CA 2011.

What Happens If No Action Is Taken?

Once the certificates expire, these failure scenarios are possible on Cisco UCS servers:

- **Windows Server fails to boot** — The UEFI firmware is unable to validate the Windows bootloader, causing Secure Boot to block the OS from loading. This affects Windows Server 2016, 2019, 2022, and 2025.
- **UEFI drivers and option ROMs are rejected** — Hardware components that rely on UEFI drivers signed with the expiring certificate can fail to initialize during POST. This could result in loss of access to RAID volumes, network connectivity during PXE boot, or other critical hardware functions.
- **Systems fall into an insecure state** — Administrators can be tempted to disable Secure Boot as a workaround, which eliminates a critical layer of firmware-level security and can violate organizational compliance policies (for example, NIST, PCI-DSS, HIPAA).
- **Large-scale operational disruption** — In enterprise environments with hundreds or thousands of UCS servers, a coordinated boot failure event could cause significant downtime across data centers.

Cisco has formally tracked this issue under **Cisco bug ID CSCwr45526**. This defect acknowledges that:

- UCS server BIOS firmware contains the expiring Microsoft 2011 Secure Boot certificates.
- A BIOS update is required to introduce the **replacement certificates (Microsoft 2023 certificates)** into the UEFI key stores.
- Without remediation, UCS servers with Secure Boot enabled are at risk of boot failures post-expiration.

Solution

Addressing this issue requires a **coordinated, two-pronged approach** — updating both the **Cisco UCS firmware (BIOS)** and the **Microsoft Windows operating system**. Neither update alone is sufficient; both sides of the Secure Boot trust chain must be modernized.

1. Apply Cisco UCS BIOS/Firmware Updates

Updated BIOS 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

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 BIOS when available for your specific UCS platform (B-Series, C-Series, X-Series).
- **Use Cisco management tools** for deployment:
  - **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.

2. Apply Microsoft Windows Updates

Microsoft is rolling out Secure Boot certificate updates through Windows Update in a phased approach:

Phase	Description	Timeline
Phase 1 — Preparation	New 2023 certificates are added to the Secure Boot **db**. Old 2011 certificates remain trusted. Both old and new certificates coexist.	**Available now**
Phase 2 —	New boot managers signed with the 2023 certificates are deployed.	**Gradual rollout**

Phase	Description	Timeline
Transition	Systems begin using the new chain of trust.	**(2025–2026)**
Phase 3 — Enforcement	Old 2011 certificates are added to the **DBX (Forbidden Signature Database)**, effectively revoking them. Only the new certificates are trusted.	**Post-expiration**

Action Steps:

- Ensure all UCS servers running Windows Server have the **latest cumulative updates** installed.
- Pay particular attention to Secure Boot–related updates in Microsoft release notes.
- **Do not skip Phase 1 and Phase 2 updates** — they are prerequisites for a smooth transition.

3. Validate the Environment

After applying both firmware and OS updates, validate the Secure Boot state on each server:

From Windows PowerShell:

powershell
Copy Code

```
# Confirm Secure Boot is active
Confirm-SecureBootUEFI

# Review Secure Boot certificate details
Get-SecureBootUEFI -Name db | Format-List
```

From Cisco IMC/Intersight:

- Verify the BIOS version reflects the updated firmware.
- Confirm Secure Boot is still **enabled** in the BIOS policy.

4. Recommended Remediation Timeline

Timeframe	Action	Priority
Now – Q2 2026	Inventory all UCS servers with Secure Boot enabled. Subscribe to updates on Cisco bug ID CSCwr45526.	High
Q2 – Q3 2026	Test updated BIOS firmware in a lab/staging environment. Apply Windows Phase 1 and Phase 2 updates.	High
Q3 2026	Begin production roll out of BIOS updates and Windows updates across UCS fleet.	High

Timeframe	Action	Priority
Before October 19, 2026	Complete all updates. Validate Secure Boot state across all servers.	Critical
Post-Expiration	Monitor for Phase 3 enforcement. Ensure no systems were missed.	Medium