Microsoft Secure Boot-Zertifikatablauf minimieren

Einleitung

In diesem Dokument wird beschrieben, wie Sie das bevorstehende Ablaufdatum von Secure Boot-Zertifikaten für Cisco UCS-Umgebungen eindämmen können.

Hintergrundinformationen

Secure Boot ist eine grundlegende Sicherheitsfunktion, die in das Unified Extensible Firmware Interface (UEFI) moderner Server und PCs integriert ist. Es stellt eine Vertrauenskette während des Bootvorgangs her, indem sichergestellt wird, dass nur digital signierte und verifizierte Software - Bootloader, Betriebssystem-Kernel und UEFI-Treiber - ausgeführt werden darf. Dieser Mechanismus schützt Systeme vor Bootkits, Rootkits und anderen Malware-Bedrohungen auf niedriger Ebene.

Das Kernstück von Secure Boot ist eine Reihe von kryptografischen Zertifikaten von Microsoft. Diese Zertifikate sind in die UEFI-Firmware praktisch aller in den letzten zehn Jahren ausgelieferten Server und PCs eingebettet, einschließlich der Cisco UCS (Unified Computing System) Server. Sie dienen als Vertrauensanker, der überprüft, ob eine Boot-Zeit-Software zulässig ist.

Microsoft hat nun bekannt gegeben, dass zwei kritische Secure Boot-Zertifikate - das Microsoft Windows Production PCA 2011 und die Microsoft UEFI CA 2011 - am 19. Oktober 2026 auslaufen werden. Dieser Ablauf betrifft das gesamte Hardware-Ökosystem, und Cisco hat die Auswirkungen auf sein UCS-Serverportfolio unter der Cisco Bug-ID CSCwr45526 anerkannt.

Problem

Welche Zertifikate laufen ab?

Die beiden Zertifikate, die im Mittelpunkt dieser Ausgabe stehen, sind:

Zertifikat	Rolle	Ablaufdatum
Microsoft Windows-Produktions-PCA 2011	Signiert und validiert Microsoft Windows-Bootloader	19. Oktober 2026
Microsoft UEFI CA 2011	Signiert und validiert UEFI-Treiber von Drittanbietern, Options-ROMs und Bootloader, die nicht von Windows stammen	19. Oktober 2026

Diese Zertifikate werden in den Secure Boot Key-Speichern der UEFI-Firmware gespeichert:

- db (Signaturdatenbank) — Enthält vertrauenswürdige Zertifikate, die zum Überprüfen von Bootzeitbinärdateien verwendet werden.
- KEK (Key Exchange Key) - Autorisiert Updates für die Signaturdatenbank.
- PK (Platform Key) - Die Vertrauensbasis, die normalerweise dem OEM (z. B. Cisco) gehört.

Welche Vorteile bieten Cisco UCS-Server?

Cisco UCS-Server - einschließlich der Plattformen B-Serie (Blade), C-Serie (Rack) und X-Serie (Modular) - werden mit diesen Microsoft 2011-Zertifikaten ausgeliefert, die in der UEFI BIOS-Firmware vorinstalliert sind. Wenn "Sicheres Booten" aktiviert ist, verwendet das BIOS diese Zertifikate bei jedem Bootvorgang, um Folgendes zu überprüfen:

1. Der Windows Server-Bootloader (z. B. `bootmgfw.efi`), der vom Windows-Produktions-PCA 2011 signiert wird.
2. UEFI-Komponenten von Drittanbietern wie:
    - Cisco VIC (Virtual Interface Card) Options-ROMs
    - Storage Controller (RAID) UEFI-Treiber
    - Netzwerkadapter PXE-Boot-ROMs
    - Beliebige andere Firmware für PCIe-Geräte, die während des POST-Tests geladen wird

    Diese werden in der Regel von der Microsoft UEFI CA 2011 unterzeichnet.

Was geschieht, wenn keine Maßnahmen ergriffen werden?

Wenn die Zertifikate ablaufen, können auf den Cisco UCS-Servern folgende Fehlerszenarien auftreten:

- Windows Server startet nicht - Die UEFI-Firmware kann den Windows-Bootloader nicht validieren, wodurch Secure Boot das Laden des Betriebssystems blockiert. Dies betrifft Windows Server 2016, 2019, 2022 und 2025.
- UEFI-Treiber und Options-ROMs werden abgelehnt - Hardwarekomponenten, die auf mit dem ablaufenden Zertifikat signierten UEFI-Treibern basieren, können während POST nicht initialisiert werden. Dies kann zu einem Verlust des Zugriffs auf RAID-Volumes, der Netzwerkverbindung während des PXE-Bootvorgangs oder anderen wichtigen Hardwarefunktionen führen.
- Systeme befinden sich in einem unsicheren Zustand - Administratoren können versucht sein, Secure Boot als Problemumgehung zu deaktivieren, wodurch eine kritische Sicherheitsebene auf Firmware-Ebene beseitigt wird und gegen Unternehmensrichtlinien (z. B. NIST, PCI-DSS, HIPAA) verstoßen werden kann.
- Umfangreiche Betriebsunterbrechungen - In Unternehmensumgebungen mit Hunderten oder Tausenden von UCS-Servern kann ein koordinierter Systemstart zu erheblichen Ausfallzeiten in den Rechenzentren führen.

Cisco hat dieses Problem offiziell unter Cisco Bug-ID CSCwr45526. Dieser Mangel bestätigt Folgendes:

- Die BIOS-Firmware des UCS-Servers enthält die ablaufenden Microsoft 2011 Secure Boot-Zertifikate.
- Ein BIOS-Update ist erforderlich, um die Ersatzzertifikate (Microsoft 2023-Zertifikate) in die UEFI-Schlüsselspeicher einzuführen.
- Ohne entsprechende Gegenmaßnahmen besteht bei UCS-Servern mit aktiviertem sicherem Booten nach Ablauf des Bootvorgangs das Risiko von Bootfehlern.

Lösung

Zur Lösung dieses Problems ist ein koordinierter, zweigleisiger Ansatz erforderlich - die Aktualisierung der Cisco UCS-Firmware (BIOS) und des Microsoft Windows-Betriebssystems. Keine Aktualisierung allein ist ausreichend; beide Seiten der Secure Boot-Vertrauenskette müssen modernisiert werden.

1. Cisco UCS BIOS-/Firmware-Updates anwenden

Aktualisierte BIOS-Firmware für betroffene UCS-Plattformen, die die neuen Microsoft Secure

Boot-Zertifikate enthält:

Neues Zertifikat	Ersetzt
Microsoft Windows UEFI CA 2023	Microsoft Windows-Produktions-PCA 2011
Microsoft UEFI CA 2023	Microsoft UEFI CA 2011

Aktionsschritte:

- Cisco Bug-ID überwachen CSCwr45526 im Cisco Bug Search Tool nach festen Firmware-Versionen und Veröffentlichungszeitplänen.
- Laden Sie das aktualisierte BIOS herunter, und stellen Sie es bereit, wenn es für Ihre spezifische UCS-Plattform (B-Serie, C-Serie, X-Serie) verfügbar ist.
- Verwenden Sie Cisco Management-Tools für die Bereitstellung:
  - Cisco Intersight - Verwenden Sie für Cloud-basierte Umgebungen Intersight-Firmware-Management-Richtlinien, um Updates skalierbar zu orchestrieren.
  - Cisco UCS Manager (UCSM) - Für Server der B- und C-Serie, die von einer Domäne verwaltet werden.
  - Cisco IMC (Integrated Management Controller) - Für eigenständige Rack-Server der C-Serie.

2. Microsoft Windows Updates anwenden

Microsoft führt Secure Boot-Zertifikataktualisierungen über Windows Update schrittweise ein:

Phase	Beschreibung	Zeitplan
Phase 1 - Vorbereitung	Neue 2023-Zertifikate werden der Secure Boot-Datenbank hinzugefügt. Alte Zertifikate von 2011 bleiben vertrauenswürdig. Sowohl alte als auch neue Zertifikate existieren nebeneinander.	Jetzt verfügbar
Phase 2 - Übergang	Es werden neue Boot-Manager bereitgestellt, die mit den 2023-Zertifikaten signiert sind. Systeme beginnen, die neue Vertrauenskette zu nutzen.	Schrittweise Einführung (2025-2026)
Phase 3 — Durchsetzung	Alte Zertifikate aus dem Jahr 2011 werden der DBX (Verbotene Signaturdatenbank) hinzugefügt, wodurch sie effektiv widerrufen werden. Nur die neuen Zertifikate sind vertrauenswürdig.	Nach Ablauf

Aktionsschritte:

- Stellen Sie sicher, dass auf allen UCS-Servern mit Windows Server die neuesten kumulativen Updates installiert sind.

- Achten Sie in den Versionshinweisen von Microsoft besonders auf Updates im Zusammenhang mit sicherem Booten.
- Überspringen Sie keine Aktualisierungen für Phase 1 und Phase 2 - sie sind Voraussetzung für einen reibungslosen Übergang.

3. Validierung der Umgebung

Nachdem Sie Firmware- und Betriebssystem-Updates angewendet haben, überprüfen Sie den Secure Boot-Status auf jedem Server:

Von Windows PowerShell aus:

Triebwerkshülse
Code kopieren

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

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

Von Cisco IMC/Intersight:

- Überprüfen Sie, ob die BIOS-Version die aktualisierte Firmware wiedergibt.
- Bestätigen Sie, dass "Sicheres Booten" weiterhin in der BIOS-Richtlinie aktiviert ist.

4. Empfohlener Behebungszeitraum

Zeitrahmen	Aktion	Priorität
Jetzt - 2. Quartal 2026	Erfassen Sie alle UCS-Server, bei denen Secure Boot aktiviert ist. Updates für Cisco Bug-ID CSCwr45526 abonnieren.	Hoch
Q2 - Q3 2026	Testen der aktualisierten BIOS-Firmware in einer Lab-/Staging-Umgebung Wenden Sie Windows Phase 1- und Phase 2-Updates an.	Hoch
3. Quartal 2026	Beginn der Implementierung von BIOS-Updates und Windows-Updates in der gesamten UCS-Produktpalette	Hoch
Vor dem 19. Oktober	Schließen Sie alle Updates ab. Überprüfen des sicheren	Critical

Zeitrahmen	Aktion	Priorität
2026	Startstatus auf allen Servern	(Kritisch)
Nach Ablauf	Überwachung der Durchsetzung von Phase 3: Stellen Sie sicher, dass keine Systeme übersehen wurden.	Mittel

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.