緩解Microsoft安全引導證書過期

簡介

本文檔介紹如何緩解安全引導證書在與Cisco UCS環境相關時即將到期的問題。

背景資訊

安全啟動是內建在現代伺服器和PC的統一可擴展韌體介面(UEFI)中的一個基礎安全功能。它通過確保僅允許執行經過數位簽章和驗證的軟體（引導載入程式、作業系統核心和UEFI驅動程式），在引導過程中建立信任鏈。此機制可保護系統免受Bootkit、Rootkit和其他低級惡意軟體威脅。

Secure Boot的核心是Microsoft頒發的一組加密證書。這些證書嵌入在過去十年中出廠的幾乎每台伺服器和PC的UEFI韌體中，包括Cisco UCS（統一計算系統）服務器。它們充當信任錨點，用於驗證引導時軟體是否合法。

Microsoft現已披露，兩個關鍵的安全引導證書(Microsoft Windows Production PCA 2011和Microsoft UEFI CA 2011)將於2026年10月19日過期。此過期影響整個硬體生態系統，思科已通過思科錯誤ID CSCwr45526確認了對UCS伺服器產品組合的影響

問題

哪些證書即將過期？

此問題的核心是以下兩個證書：

憑證	角色	到期日期
Microsoft Windows生產PCA 2011	簽名並驗證Microsoft Windows載入程式	2026年10月19日
Microsoft UEFI CA 2011	簽名並驗證第三方UEFI驅動程式、選項ROM和非Windows載入程式	2026年10月19日

這些證書儲存在UEFI韌體安全啟動金鑰儲存區中:

- db（簽名資料庫） — 包含用於驗證啟動時間二進位制檔案的受信任證書。
- KEK（金鑰交換金鑰） — 授權對簽名資料庫的更新。
- PK(平台金鑰) — 信任的根，通常由OEM（例如，思科）擁有。

為什麼這是Cisco UCS伺服器的問題？

Cisco UCS伺服器(包括B系列（刀片）、C系列（機架）和X系列（模組化）平台)附帶預載入到其UEFI BIOS韌體中的Microsoft 2011證書。啟用安全引導後，BIOS會在每個引導週期使用這些證書進行驗證：

1. Windows Server引導載入程式(例如，`bootmgfw.efi`) — 由Windows Production PCA 2011簽名。
2. 第三方UEFI元件，如：
   - Cisco VIC（虛擬介面卡）選項ROM
   - 儲存控制器(RAID)UEFI驅動程式
   - 網路介面卡PXE引導ROM
   - POST期間載入的任何其他PCIe裝置韌體

   通常由Microsoft UEFI CA 2011簽署。

如果不執行任何操作會發生什麼情況？

證書到期後，思科UCS伺服器上可能出現以下故障情況：

- Windows Server fails to boot - UEFI韌體無法驗證Windows引導載入程式，從而導致安全引導阻止載入作業系統。這將影響Windows Server 2016、2019、2022和2025。
- UEFI驅動程式和選項ROM被拒絕 — 依賴使用過期證書簽名的UEFI驅動程式的硬體元件在POST期間可能無法初始化。這可能會導致無法訪問RAID卷、在PXE啟動期間的網路連線或其他關鍵硬體功能。
- 系統進入不安全狀態 — 管理員可能會傾向於禁用安全引導作為解決方案，從而消除韌體級別安全性的關鍵層，並可能違反組織合規性策略（例如NIST、PCI-DSS、HIPAA）。
- 大規模運營中斷 — 在擁有數百或數千台UCS伺服器的企業環境中，協調引導故障事件可能會導致資料中心出現大量停機。

思科已正式跟蹤此問題，其網址為 思科錯誤ID CSCwr45526 .此缺陷承認：

- UCS伺服器BIOS韌體包含即將到期的Microsoft 2011安全引導證書。
- 需要更新BIOS才能將替換證書（Microsoft 2023證書）引入到UEFI金鑰庫。
- 如果不進行修復，啟用安全引導的UCS伺服器在到期後會有引導失敗的風險。

解決方案

解決此問題需要協調的雙管齊下方法 — 更新Cisco UCS韌體(BIOS)和Microsoft Windows作業系統。僅更新一項是不夠的；安全啟動信任鏈的兩端都必須進行現代化。

1.應用Cisco UCS BIOS/韌體更新

已更新受影響的UCS平台的BIOS韌體，包括新的Microsoft安全引導證書：

新證書	替換
Microsoft Windows UEFI CA 2023	Microsoft Windows生產PCA 2011
Microsoft UEFI CA 2023	Microsoft UEFI CA 2011

操作步驟：

- 監控思科錯誤ID CSCwr45526 ，瞭解固定韌體版本和版本的時間表。
- 下載並部署更新的BIOS(適用於您的特定UCS平台（B系列、C系列和X系列）。
- 使用思科管理工具進行部署：
  - Cisco Intersight -對於雲託管環境，請使用Intersight韌體管理策略來大規模協調更新。
  - Cisco UCS Manager(UCSM) — 用於域管理的B系列和C系列伺服器。
  - 思科IMC（整合管理控制器） — 適用於獨立C系列機架式伺服器。

2.應用Microsoft Windows更新

Microsoft正在分階段通過Windows Update推出安全引導證書更新：

Phase	說明	時間表
第1階段 — 準備	新的2023證書將新增到安全引導資料庫。舊的2011證書仍然受信任。新舊憑證共存。	現已推出
第2階段 — 過渡	部署使用2023證書簽署的新引導管理器。系統開始使用新的信任鏈。	逐步推廣（2025-2026年）
第3階段 —	舊的2011證書被新增到DBX(禁止簽名資料庫),有效地撤消它們	過期後

Phase	說明	時間表
實施	。僅信任新證書。	

操作步驟：

- 確保運行Windows Server的所有UCS伺服器都安裝了最新的累積更新。
- 請特別注意Microsoft發行說明中與安全啟動相關的更新。
- 不要跳過第1階段和第2階段更新— — 它們是平穩過渡的前提條件。

3.驗證環境

應用韌體和作業系統更新後，驗證每台伺服器上的安全引導狀態：

在Windows PowerShell中：

powershell
複製代碼

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

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

在Cisco IMC/Intersight上：

- 驗證BIOS版本是否反映更新的韌體。
- 確認BIOS策略中仍啟用「Secure Boot（安全啟動）」。

4.建議的補救時間表

時間範圍	動作	優先順序機制
現在 — 2026年第2季度	清點啟用安全引導的所有UCS伺服器。訂閱思科錯誤ID CSCwr45526的更新.	高
2026年第二季度 —	在實驗/試運行環境中測試更新的BIOS韌體。應用Windows第1階段和	高

時間範圍	動作	優先順序機制
第三季度	第2階段的更新。	
2026年第3季度	開始在UCS車隊中推廣BIOS更新和Windows更新。	高
2026年10月19日之前	完成所有更新。跨所有伺服器驗證安全引導狀態。	嚴重
過期後	監控第3階段的實施。確保未丟失任何系統。	中

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。