缓解Microsoft安全引导证书过期

简介

本文档介绍如何缓解安全引导证书即将到期的问题，因为它适用于Cisco UCS环境。

背景信息

安全引导是内置在现代服务器和PC的统一可扩展固件接口(UEFI)中的一项基本安全功能。它通过确保仅允许执行经过数字签名和验证的软件（引导加载程序、操作系统内核和UEFI驱动程序），在引导过程中建立信任链。此机制可保护系统免受Bootkit、Rootkit和其他低级恶意软件威胁。

Secure Boot的核心是Microsoft颁发的一组加密证书。在过去十年中，这些证书几乎嵌入到所有服务器和PC的UEFI固件中，包括Cisco UCS（统一计算系统）服务器。它们充当信任锚，用于验证引导时软件是否合法。

Microsoft现已披露，两个关键安全引导证书(Microsoft Windows Production PCA 2011和Microsoft UEFI CA 2011)将于2026年10月19日到期。此过期会影响整个硬件生态系统，思科已通过Cisco Bug ID CSCwr确认了UCS服务器产品组合的影响45526

问题

哪些证书即将过期？

此问题的核心是以下两个证书：

证书	角色	到期日期
Microsoft Windows生产PCA 2011	签名并验证Microsoft Windows引导程序	2026年10月19日
Microsoft UEFI CA 2011	签名并验证第三方UEFI驱动程序、选项ROM和非Windows引导程序	2026年10月19日

这些证书存储在UEFI固件安全启动密钥存储中:

- db（签名数据库） — 包含用于验证引导时二进制文件的受信任证书。
- KEK（密钥交换密钥） — 授权对签名数据库的更新。
- PK(平台密钥) — 信任的根，通常由OEM（例如思科）拥有。

为什么这是Cisco UCS服务器的问题？

Cisco UCS服务器(包括B系列（刀片）、C系列（机架）和X系列（模块化）平台)随附预加载到其UEFI BIOS固件中的Microsoft 2011证书。启用安全引导后，BIOS会在每个引导周期使用这些证书进行验证：

1. Windows Server bootloader(例如，`bootmgfw.efi`) — 由Windows Production PCA 2011签名。
2. 第三方UEFI组件，例如：
    - Cisco VIC（虚拟接口卡）选项ROM
    - 存储控制器(RAID)UEFI驱动程序
    - 网络适配器PXE引导ROM
    - POST期间加载的任何其他PCIe设备固件

    这些证书通常由Microsoft UEFI CA 2011签署。

如果不执行操作会发生什么情况？

证书到期后，Cisco UCS服务器上可能出现以下故障情况：

- Windows Server fails to boot — UEFI固件无法验证Windows引导加载程序，导致安全引导阻止加载操作系统。这会影响Windows Server 2016、2019、2022和2025。
- UEFI驱动程序和选项ROM被拒绝 — 依赖使用过期证书签名的UEFI驱动程序的硬件组件在POST期间可能无法初始化。这可能导致无法访问RAID卷、在PXE引导期间网络连接或其他关键硬件功能。
- 系统处于不安全状态 — 管理员可能会忍不住禁用安全引导作为应急方案，从而消除固件级别安全性的关键层，并可能违反组织合规性策略（例如，NIST、PCI-DSS、HIPAA）。
- 大规模运营中断 — 在拥有数百或数千台UCS服务器的企业环境中，一次协调的引导故障事件可能会导致数据中心出现大量停机时间。

思科已正式跟踪此问题，其网址为 思科漏洞ID CSCwr45526 .此缺陷承认：

- UCS服务器BIOS固件包含即将到期的Microsoft 2011安全引导证书。
- 需要进行BIOS更新，以将替换证书（Microsoft 2023证书）引入到UEFI密钥库中。
- 如果不进行修复，启用安全引导的UCS服务器在到期后有引导失败的风险。

解决方案

解决此问题需要一种协调的双管齐下方法 — 更新Cisco UCS固件(BIOS)和Microsoft Windows操作系统。仅更新一项是不够的；安全启动信任链的两端都必须进行现代化。

1.应用Cisco UCS BIOS/固件更新

已更新受影响的UCS平台的BIOS固件，包括新的Microsoft安全引导证书：

新证书	替换
Microsoft Windows UEFI CA 2023	Microsoft Windows生产PCA 2011
Microsoft UEFI CA 2023	Microsoft UEFI CA 2011

操作步骤：

- 监控Cisco Bug ID CSCwr45526 在Cisco Bug Search Tool上查找固定固件版本和版本时间表。
- 下载并部署更新的BIOS(适用于您的特定UCS平台（B系列、C系列、X系列）。
- 使用思科管理工具进行部署：
  - Cisco Intersight -对于云托管环境，请使用Intersight固件管理策略大规模协调更新。
  - Cisco UCS Manager(UCSM)-用于域管理的B系列和C系列服务器。
  - 思科IMC(集成管理控制器) — 适用于独立C系列机架式服务器。

2.应用Microsoft Windows更新

Microsoft正在分阶段地通过Windows Update推出安全引导证书更新：

阶段	描述	时间表
第1阶段 — 准备	新的2023证书将添加到安全引导db中。旧的2011证书仍然受信任。新旧证书共存。	现已推出
第2阶段 — 过渡	部署使用2023证书签名的新引导管理器。系统开始使用新的信任链。	逐步推广（2025-2026年）

阶段	描述	时间表
第3阶段 — 实施	旧2011证书将添加到DBX(禁止签名数据库)，从而有效地撤销这些证书。仅信任新证书。	过期后

操作步骤：

- 确保运行Windows Server的所有UCS服务器都安装了最新的累积更新。
- 请特别注意Microsoft发行说明中与安全引导相关的更新。
- 不要跳过第1阶段和第2阶段的更新 — 它们是平稳过渡的前提条件。

3.验证环境

应用固件和操作系统更新后，验证每台服务器上的安全引导状态：

在Windows PowerShell中：

powershell
复制代码

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

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

从Cisco IMC/Intersight:

- 验证BIOS版本是否反映更新的固件。
- 在BIOS策略中确认安全引导仍启用。

4.建议的补救时间表

时间段	操作	优先级
现在 — 2026年第2季度	清点启用安全引导的所有UCS服务器。订阅有关Cisco Bug ID CSCwr45526的更新.	高
2026年第二季度 —	在实验/试运行环境中测试更新的BIOS固件。应用Windows第1阶段和	高

时间段	操作	优先级
第三季度	第2阶段的更新。	
2026年三季度	开始在UCS群中部署BIOS更新和Windows更新。	高
2026年10月19日前	完成所有更新。跨所有服务器验证安全引导状态。	关键
过期后	监控第3阶段的实施。确保未丢失任何系统。	中

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。