缓解Microsoft安全引导证书过期

目录

简介

背景信息

问题

- 哪些证书即将过期？
- 为什么这是Cisco UCS服务器的问题？
- 如果不执行操作会发生什么情况？

解决方案

- 应用Cisco UCS固件更新
- 操作步骤
- Intersight管理模式(IMM) — 服务器
  - 刀片服务器（B和X — 系列）
  - 集成在深入分析管理模式(IMC)中的机架式服务器（C系列）
- 独立机架式服务器（C系列）— 主机升级实用程序(HUU)
- UCS Manager(UCSM) — 托管服务器

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

安全启动是内置在现代服务器和PC的统一可扩展固件接口(UEFI)中的基本安全功能。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，关键安全引导证书将于2026年6月到期。此过期会影响整个硬件生态系统，思科已通过Cisco Bug ID CSCwr45526确认了UCS服务器产品组合受到的影响。

问题

哪些证书即将过期？

此问题的核心是以下三个证书：

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6月27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6月27日
Microsoft Corporation KEK CA 2011	将更新签到DB和DBX。	2026年6月24日

这些证书存储在UEFI固件安全引导密钥库中：

- 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 — 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安全引导证书。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：

- 操作系统引导加载程序，由Windows Production PCA 2011签名。
- 第三方UEFI组件，例如：
  - 存储控制器(RAID)UEFI驱动程序
  - 网络适配器PXE引导ROM
  - POST期间加载的其他PCIe设备固件

这些组件通常由Microsoft UEFI CA 2011签名。

如果不执行操作会发生什么情况？

- 现有的操作系统、驱动程序和选项ROM继续正常运行，因为它们使用当前受信任证书进行签名，并且不依赖于新的证书颁发机构。因此，受影响的服务器将继续启动，而不会中断。到期仅影响未来使用新证书签名的二进制文件，不会追溯性地使之前已签名和已受信任的组件失效。
- 使用新证书重新签名文件的点由负责每个组件的供应商确定，而不是由单个协调事件确定。这同样适用于基于UCS的设备，其时间表由负责这些映像的各供应商和签署机构管理。
- 这不是Windows特有的问题。依赖安全引导并采用新签名证书的任何操作系统或固件组件都遵循随时间推移的相同过渡要求。因此，与负责任的设备供应商进行协调至关重要。将直接跟踪每个供应商发布的指南和公告，而不是假设仅基础的UCS固件更新就足够了，因为设备操作系统映像签名与平台固件分开控制。

此表基于CIMC证书状态以及是否启用安全引导概述了预期引导行为。它说明需要补救（将CIMC更新为新证书）才能保持引导未来签名文件的能力：

CIMC证书状态	安全启动已启用	安全启动已启用 —	已禁用安全启动	已禁用安全启动
	当前文件	将来的文件	当前文件	将来的文件
旧CIMC（旧证书）	O	X	O	O
新CIMC（新认证）	O	O	O	O

图例：O =成功启动· X =启动失败/不受信任的文件

思科已正式在Cisco Bug ID CSCwr45526下跟踪此问题。

此缺陷承认：

- UCS服务器固件包含即将到期的Microsoft 2011安全引导证书。
- 需要固件更新以将替换证书（Microsoft 2023证书）引入到UEFI密钥库中。

注：如果UCS服务器在传统引导模式下运行，则不会发生安全引导证书问题。同样，禁用安全引导的UEFI模式不会受到影响。

解决方案

应用Cisco UCS固件更新

已更新受影响的UCS平台的固件，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
Microsoft Corporation KEK 2K CA 2023	Microsoft Corporation KEK CA 2011

操作步骤

- 在Cisco Bug Search Tool上监控Cisco Bug ID CSCwr4526，了解固定固件版本和版本时间表。
- 下载并部署更新后的固件(适用于您的特定UCS平台（B系列、C系列和X系列）。
- 使用思科管理工具进行固件升级：
  - 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） — 用于独立的C系列机架式服务器。

接下来的表格包含最低固件版本，其中包含具有更新证书的修补程序，更高版本也包含修补程序：

Intersight管理模式(IMM) — 服务器

刀片服务器（B和X — 系列）

服务器型号	固件版本
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

集成在Insight管理模式(IMC)中的机架式服务器（C系列）

IMC固件版本
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

独立机架式服务器（C系列） — 主机升级实用程序(HUU)

服务器型号	固件版本
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) — 托管服务器

UCSM固件版本
4.3(6f)
6.0(2b)

根据UCS服务器上的操作系统，解决UEFI证书过期问题有时需要额外的配置。思科建议联系各操作

系统供应商，获取有关具体补救步骤的指导。



注意：仅UCS服务器上的固件更新并不总是能完全解决此问题。操作系统级证书更新也可能是必要的，以确保在2026年UEFI证书到期日期之后继续使用安全引导功能。

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）。