Microsoft 보안 부팅 인증서 만료 완화

소개

이 문서에서는 Cisco UCS 환경과 관련된 보안 부팅 인증서의 만료를 줄이는 방법에 대해 설명합니다.

배경 정보

보안 부팅은 최신 서버 및 PC의 UEFI(Unified Extensible Firmware Interface)에 내장된 기본 보안 기능입니다. 부팅 과정에서 디지털 서명 및 확인된 소프트웨어(부트로더, 운영 체제 커널, UEFI 드라이버)만 실행할 수 있도록 하여 신뢰 체인을 설정합니다. 이 메커니즘은 부트킷, 루트킷 및 기타 하위 레벨 악성코드 위협으로부터 시스템을 보호합니다.

보안 부팅의 중심에는 Microsoft에서 발급한 암호화 인증서 집합이 있습니다. 이러한 인증서는 Cisco UCS(Unified Computing System) 서버를 비롯하여 지난 10년 동안 출하된 거의 모든 서버 및 PC의 UEFI 펌웨어에 내장됩니다. 이들은 부트 시간 소프트웨어의 일부가 합법적인지 여부를 검증하는 트러스트 앵커 역할을 합니다.

Microsoft는 이제 두 가지 중요한 보안 부팅 인증서(Microsoft Windows Production PCA 2011 및 Microsoft UEFI CA 2011)가 2026년 10월 19일에 만료된다고 밝혔습니다. 이 만료는 전체 하드웨어 에코시스템에 영향을 미치며, Cisco는 Cisco 버그 ID CSCwr에 따라 UCS 서버 포트폴리오에 미치는 영향을 인정했습니다45526

문제

어떤 인증서가 만료됩니까?

이 문제의 중심에 있는 두 인증서는 다음과 같습니다.

인증서	역할	만료 날짜
Microsoft Windows 프로덕션 PCA 2011	Microsoft Windows 부트로더 서명 및 유효성 검사	2026년 10월 19일
Microsoft UEFI CA 2011	타사 UEFI 드라이버, 옵션 ROM 및 비 Windows 부트로더 서명 및 검증	2026년 10월 19일

이러한 인증서는 UEFI 펌웨어 보안 부팅 키 저장소에 저장됩니다.

- db(시그니처 데이터베이스) — 부트 시간 이진 파일을 확인하는 데 사용되는 신뢰할 수 있는 인증서를 포함합니다.
- KEK(키 교환 키) — 서명 데이터베이스에 대한 업데이트를 승인합니다.
- PK(Platform Key) — 일반적으로 OEM(예: Cisco)이 소유하는 신뢰의 루트입니다.

Cisco UCS Server에서 이 문제가 발생하는 이유는 무엇입니까?

B-Series(Blade), C-Series(Rack), X-Series(Modular) 플랫폼을 비롯한 Cisco UCS 서버는 UEFI BIOS 펌웨어에 사전 로드된 Microsoft 2011 인증서와 함께 제공됩니다. 보안 부팅이 활성화되면 BIOS는 부팅 주기마다 다음 인증서를 사용하여 다음을 검증합니다.

1. Windows Server 부트로더(예: `bootmgfw.efi`) - Windows Production PCA 2011에서 서명했습니다.
2. 서드파티 UEFI 구성 요소:
   - Cisco VIC(Virtual Interface Card) 옵션 ROM
   - 스토리지 컨트롤러(RAID) UEFI 드라이버
   - 네트워크 어댑터 PXE 부팅 ROM
   - POST 중에 로드된 다른 모든 PCIe 디바이스 펌웨어

   일반적으로 Microsoft UEFI CA 2011에서 서명합니다.

아무 조치도 취해지지 않으면 어떻게 됩니까?

인증서가 만료되면 Cisco UCS 서버에서 다음과 같은 실패 시나리오를 수행할 수 있습니다.

- Windows Server 부팅 실패 — UEFI 펌웨어가 Windows 부트로더를 검증할 수 없으므로 보안 부팅이 OS 로드를 차단합니다. 이는 Windows Server 2016, 2019, 2022 및 2025에 영향을 줍니다.
- UEFI 드라이버 및 옵션 ROM이 거부됨 - 만료 예정인 인증서로 서명된 UEFI 드라이버에 의존하는 하드웨어 구성 요소가 POST 중에 초기화하지 못할 수 있습니다. 이로 인해 RAID 볼륨에 대한 액세스, PXE 부팅 중 네트워크 연결 또는 기타 중요한 하드웨어 기능이 손실될 수 있습니다.

- 시스템이 안전하지 않은 상태로 빠짐 - 관리자가 보안 부팅을 사용하지 않도록 설정하려는 유혹을 받을 수 있습니다. 그러면 중요한 펌웨어 수준 보안 레이어가 제거되고 조직의 규정 준수 정책(예: NIST, PCI-DSS, HIPAA)을 위반할 수 있습니다.
- 대규모 운영 중단 — 수백 또는 수천 대의 UCS 서버가 설치된 엔터프라이즈 환경에서 부팅 실패 시 데이터 센터 전반에서 심각한 다운타임이 발생할 수 있습니다.

Cisco는 공식적으로 Cisco 버그 ID CSCwr45526. 이 결함은 다음을 인정합니다.

- UCS 서버 BIOS 펌웨어는 만료되는 Microsoft 2011 Secure Boot 인증서를 포함합니다.
- 대체 인증서(Microsoft 2023 인증서)를 UEFI 키 저장소에 도입하려면 BIOS 업데이트가 필요합니다.
- 보안 부팅이 활성화된 UCS 서버는 리미디에이션이 없으면 만료 후 부팅 실패의 위험이 있습니다.

솔루션

이 문제를 해결하려면 Cisco UCS 펌웨어(BIOS)와 Microsoft Windows 운영 체제를 모두 업데이트하는 조율된 두 갈래 접근 방식이 필요합니다. 업데이트만으로는 충분하지 않습니다. 보안 부팅 신뢰 체인의 양쪽을 현대화해야 합니다.

1. Cisco UCS BIOS/펌웨어 업데이트 적용

새 Microsoft Secure Boot 인증서가 포함된 영향을 받는 UCS 플랫폼의 BIOS 펌웨어 업데이트:

새 인증서	대체
Microsoft Windows UEFI CA 2023	Microsoft Windows 프로덕션 PCA 2011
Microsoft UEFI CA 2023	Microsoft UEFI CA 2011

작업 단계:

- Cisco 버그 ID CSCwr 모니터링45526 고정 펌웨어 버전 및 릴리스 일정에 대한 Cisco Bug Search Tool의 경우
- 특정 UCS 플랫폼(B-Series, C-Series, X-Series)에서 사용 가능한 경우 업데이트된 BIOS를 다운로드하고 구축합니다.
- 구축에 Cisco 관리 툴 사용:
  - Cisco Intersight — 클라우드 매니지드 환경의 경우, Intersight 펌웨어 관리 정책을 사용하여 규모에 맞게 업데이트를 오케스트레이션합니다.

- Cisco UCSM(UCS Manager) - 도메인 관리 B-Series 및 C-Series 서버용.
- Cisco IMC(Integrated Management Controller) - 독립형 C-Series 랙 서버용

2. Microsoft Windows 업데이트 적용

Microsoft는 Windows 업데이트를 통해 보안 부팅 인증서 업데이트를 단계적으로 배포하고 있습니다.

단계	설명	일정
1단계 - 준비	새 2023 인증서가 Secure Boot DB에 추가됩니다. 이전 2011 인증서는 신뢰할 수 있습니다. 기존 인증서와 새 인증서가 모두 공존합니다.	현재 사용 가능
2단계 - 전환	2023 인증서로 서명된 새 부트 관리자가 구축됩니다. 시스템은 새로운 신뢰 체인을 사용하기 시작합니다.	점진적 출시 (2025-2026)
3단계 - 시행	이전 2011 인증서는 DBX(Forbidden Signature Database)에 추가되어 사실상 폐기됩니다. 새 인증서만 신뢰할 수 있습니다.	만료 후

작업 단계:

- Windows Server를 실행하는 모든 UCS 서버에 최신 누적 업데이트가 설치되어 있는지 확인합니다.
- Microsoft 릴리스 노트의 보안 부팅 관련 업데이트에 특히 주의하십시오.
- 1단계 및 2단계 업데이트를 건너뛰지 마십시오. 원활한 전환을 위한 전제 조건입니다.

3. 환경 검증

펌웨어 및 OS 업데이트를 모두 적용한 후 각 서버에서 보안 부팅 상태를 확인합니다.

Windows PowerShell에서:

PowerShell
코드 복사

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

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

Cisco IMC/Intersight에서:

- BIOS 버전이 업데이트된 펌웨어를 반영하는지 확인합니다.
- 보안 부팅이 BIOS 정책에서 여전히 활성화되었는지 확인합니다.

4. 권장 리미디에이션 일정

기간	작업	우선순위
현재 - 2026년 2분기	보안 부팅이 활성화된 모든 UCS 서버를 인벤토리화합니다. Cisco 버그 ID CSCwr에 대한 업데이트를 구독하십시오45526.	높음
2026년 2분기 - 3분기	랩/스테이징 환경에서 업데이트된 BIOS 펌웨어를 테스트합니다. Windows 1단계 및 2단계 업데이트를 적용합니다.	높음
2026년 3분기	UCS 플릿에서 BIOS 업데이트 및 Windows 업데이트의 프로덕션 롤아웃을 시작합니다.	높음
2026년 10월 19일 이전	모든 업데이트를 완료합니다. 모든 서버에서 보안 부팅 상태를 확인합니다.	Critical(심각)
만료 후	3단계 시행 모니터링 누락된 시스템이 없는지 확인합니다.	중간

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.