Riduci scadenza certificato di avvio protetto Microsoft

Introduzione

In questo documento viene descritto come limitare l'imminente scadenza dei certificati di avvio protetto per quanto riguarda gli ambienti Cisco UCS.

Premesse

Secure Boot è una funzione di sicurezza di base integrata nell'interfaccia UEFI (Unified Extensible Firmware Interface) dei server e dei PC moderni. Stabilisce una catena di attendibilità durante il processo di avvio garantendo che solo il software con firma digitale e verificato (bootloader, kernel del sistema operativo e driver UEFI) possa essere eseguito. Questo meccanismo protegge i sistemi da bootkit, rootkit e altre minacce malware di basso livello.

Alla base di Secure Boot vi è un insieme di certificati crittografici emessi da Microsoft. Questi certificati sono integrati nel firmware UEFI di praticamente tutti i server e i PC forniti nell'ultimo decennio, inclusi i server Cisco UCS (Unified Computing System). Fungono da trust anchor che convalidano la legittimità di un software di avvio.

Microsoft ha annunciato che due certificati critici per l'avvio protetto, Microsoft Windows Production PCA 2011 e Microsoft UEFI CA 2011, scadranno il 19 ottobre 2026. Questa scadenza influisce sull'intero ecosistema hardware e Cisco ha riconosciuto l'impatto sul proprio portafoglio di server UCS con l'ID bug Cisco CSCwr45526

Problema

Quali certificati sono in scadenza?

I due certificati al centro di questo problema sono:

Certificato	Ruolo	Data di scadenza
Microsoft Windows	Firma e convalida i caricatori di avvio di Microsoft	19 ottobre

Certificato	Ruolo	Data di scadenza
Production APC 2011	Windows	2026
Microsoft UEFI CA 2011	Firma e convalida i driver UEFI di terze parti, le Option ROM e i bootloader non Windows	19 ottobre 2026

Questi certificati sono archiviati negli archivi chiavi di avvio protetto del firmware UEFI:

- db (database delle firme): contiene i certificati attendibili utilizzati per verificare i file binari della fase di avvio.
- KEK (chiave di scambio chiave): autorizza gli aggiornamenti al database delle firme.
- PK (Platform Key): la radice del trust, in genere di proprietà dell'OEM, ad esempio Cisco.

Perché si tratta di un problema per i server Cisco UCS?

I server Cisco UCS, incluse le piattaforme serie B (Blade), serie C (Rack) e serie X (Modular), sono forniti con questi certificati Microsoft 2011 precaricati nel firmware del BIOS UEFI. Quando l'opzione Secure Boot è abilitata, il BIOS utilizza questi certificati ad ogni ciclo di avvio per convalidare:

1. Il bootloader di Windows Server (ad esempio, `bootmgfw.efi`), firmato da Windows Production PCA 2011.
2. Componenti UEFI di terze parti quali:
   - ROM opzionali Cisco VIC (Virtual Interface Card)
   - Driver UEFI per controller di storage (RAID)
   - ROM di avvio PXE della scheda di rete
   - Qualsiasi altro firmware di dispositivo PCIe caricato durante il POST

   In genere sono firmati dalla CA 2011 Microsoft UEFI.

Cosa Succede Se Non Viene Intrapresa Alcuna Azione?

Una volta scaduti i certificati, sui server Cisco UCS sono possibili i seguenti scenari di errore:

- Impossibile avviare Windows Server — Il firmware UEFI non è in grado di convalidare il bootloader di Windows, causando il blocco del caricamento del sistema operativo da parte di

Secure Boot. Questo influisce su Windows Server 2016, 2019, 2022 e 2025.

- I driver UEFI e le Option ROM sono rifiutati — I componenti hardware che si basano su driver UEFI firmati con il certificato in scadenza potrebbero non essere inizializzati durante il POST. Ciò potrebbe causare la perdita dell'accesso ai volumi RAID, la connettività di rete durante l'avvio PXE o altre funzioni hardware critiche.
- I sistemi non sono sicuri: gli amministratori possono essere tentati di disabilitare l'avvio protetto come soluzione alternativa, eliminando un livello critico di sicurezza a livello di firmware e violando le policy aziendali di conformità (ad esempio, NIST, PCI-DSS, HIPAA).
- Interruzione delle attività su larga scala: negli ambienti aziendali con centinaia o migliaia di server UCS, un errore di avvio coordinato potrebbe causare tempi di inattività significativi nei data center.

Cisco ha registrato formalmente questo problema in ID bug Cisco CSCwr4526. Questo difetto riconosce che:

- Il firmware del BIOS del server UCS contiene i certificati di avvio protetto di Microsoft 2011 in scadenza.
- È necessario un aggiornamento del BIOS per introdurre i certificati sostitutivi (certificati Microsoft 2023) negli archivi chiavi UEFI.
- Senza la risoluzione dei problemi, i server UCS con Secure Boot abilitato sono a rischio di errori di avvio dopo la scadenza.

Soluzione

Per risolvere questo problema è necessario un approccio coordinato e su due livelli: aggiornare il firmware (BIOS) e il sistema operativo Microsoft Windows di Cisco UCS. Nessun aggiornamento da solo è sufficiente; è necessario modernizzare entrambi i lati della catena di attendibilità dell'avvio protetto.

1. Applicazione degli aggiornamenti di Cisco UCS BIOS/firmware

Firmware del BIOS aggiornato per le piattaforme UCS interessate che include i nuovi certificati Microsoft Secure Boot:

Nuovo certificato	Sostituisce
Microsoft Windows UEFI CA 2023	Microsoft Windows Production APC 2011
Microsoft UEFI CA 2023	Microsoft UEFI CA 2011

Passaggi azione:

- Monitoraggio ID bug Cisco CSCwr4526 su Cisco Bug Search Tool per le versioni del firmware e le timeline delle versioni fisse.
- Scaricare e distribuire il BIOS aggiornato quando disponibile per la piattaforma UCS specifica (serie B, serie C, serie X).
- Utilizzare gli strumenti di gestione Cisco per l'installazione:
  - Cisco Intersight: per gli ambienti gestiti tramite cloud, utilizzare le policy di gestione del firmware Intersight per gestire gli aggiornamenti in modo scalabile.
  - Cisco UCS Manager (UCSM): per server serie B e serie C gestiti dal dominio.
  - Cisco IMC (Integrated Management Controller): per server rack standalone serie C.

2. Applicare gli aggiornamenti di Microsoft Windows

Microsoft sta implementando gli aggiornamenti dei certificati di avvio protetto tramite Windows Update in un approccio in più fasi:

Fase	Descrizione	Cronologia
Fase 1 — Preparazione	I nuovi certificati 2023 vengono aggiunti al database di avvio protetto. I certificati precedenti del 2011 rimangono attendibili. I certificati vecchi e nuovi coesistono.	Disponibile ora
Fase 2 — Transizione	Vengono distribuiti nuovi boot manager firmati con i certificati 2023. I sistemi iniziano a utilizzare la nuova catena di fiducia.	Implementazione graduale (2025-2026)
Fase 3 — Applicazione	I certificati precedenti del 2011 vengono aggiunti al database DBX (Forbidden Signature), revocandoli di fatto. Solo i nuovi certificati sono attendibili.	Post-scadenza

Passaggi azione:

- Verificare che in tutti i server UCS che eseguono Windows Server siano installati gli aggiornamenti cumulativi più recenti.
- Prestare particolare attenzione agli aggiornamenti relativi all'avvio protetto nelle note sulla versione di Microsoft.
- Non ignorare gli aggiornamenti di Fase 1 e Fase 2, in quanto costituiscono i prerequisiti per una transizione senza problemi.

3. Convalida dell'ambiente

Dopo aver applicato gli aggiornamenti del firmware e del sistema operativo, convalidare lo stato di avvio protetto su ciascun server:

Da Windows PowerShell:

powershell
Copia codice

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

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

Da Cisco IMC/Intersight:

- Verificare che la versione del BIOS rifletta il firmware aggiornato.
- Confermare che l'avvio protetto è ancora abilitato nei criteri del BIOS.

4. Tempi di risoluzione consigliati

Tempi	Azione	Priority
Ora - secondo trimestre 2026	Eseguire l'inventario di tutti i server UCS con l'avvio protetto abilitato. Iscriviti agli aggiornamenti sull'ID bug Cisco CSCwr45526 .	Alta
T2 - T3 2026	Testare il firmware aggiornato del BIOS in un ambiente lab/staging. Applicare gli aggiornamenti di Windows fase 1 e fase 2.	Alta
T3 2026	Inizio dell'implementazione di produzione degli aggiornamenti del BIOS e di Windows nel parco UCS.	Alta
Prima del 19 ottobre 2026	Completare tutti gli aggiornamenti. Convalidare lo stato di avvio protetto in tutti i server.	Critico
Post-scadenza	Monitorare l'applicazione della fase 3. Accertarsi che non vi siano sistemi mancanti.	Media

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).