Vervaldatum Microsoft Secure Boot Certificate beperken

Inleiding

In dit document wordt beschreven hoe u de komende vervaldatum van Secure Boot Certificates kunt beperken, aangezien deze betrekking heeft op Cisco UCS-omgevingen.

Achtergrondinformatie

Secure Boot is een fundamentele beveiligingsfunctie die is ingebouwd in de Unified Extensible Firmware Interface (UEFI) van moderne servers en pc's. Het creëert een keten van vertrouwen tijdens het opstartproces door ervoor te zorgen dat alleen digitaal ondertekende en geverifieerde software - bootloaders, kernels van het besturingssysteem en UEFI-stuurprogramma's - mogen worden uitgevoerd. Dit mechanisme beschermt systemen tegen bootkits, rootkits en andere malware-bedreigingen op laag niveau.

Het hart van Secure Boot ligt een set cryptografische certificaten uitgegeven door Microsoft. Deze certificaten zijn ingebed in de UEFI-firmware van vrijwel elke server en pc die de afgelopen tien jaar is geleverd, inclusief Cisco UCS-servers (Unified Computing System). Ze dienen als de vertrouwensankers die valideren of een stukje opstarttijd-software legitiem is.

Microsoft heeft nu bekendgemaakt dat twee kritieke Secure Boot-certificaten - de Microsoft Windows Production PCA 2011 en de Microsoft UEFI CA 2011 - op 19 oktober 2026 zullen vervallen. Deze vervaldatum is van invloed op het hele hardware-ecosysteem en Cisco heeft de impact op zijn UCS-serverportfolio erkend onder Cisco-bug-ID CSCwr45526

Probleem

Welke certificaten verlopen?

De twee certificaten die centraal staan in deze uitgifte zijn:

getuigschrift	rol	Vervaldatum
Microsoft Windows	Microsoft Windows-bootloaders ondertekenen en	19 oktober

getuigschrift	rol	Vervaldatum
Production PCA 2011	valideren	2026
Microsoft UEFI CA 2011	UEFI-stuurprogramma's van derden, optie-ROM's en niet-Windows-bootloaders ondertekenen en valideren	19 oktober 2026

Deze certificaten worden opgeslagen in de UEFI firmware Secure Boot key stores:

- db (Signature Database) — Bevat vertrouwde certificaten die worden gebruikt om opstarttijden-binaries te verifiëren.
- KEK (Key Exchange Key) — autoriseert updates van de Handtekeningendatabase.
- PK (Platform Key) — De basis van vertrouwen, meestal eigendom van de OEM (bijvoorbeeld Cisco).

Waarom is dit een probleem voor Cisco UCS-servers?

Cisco UCS-servers — waaronder de B-reeks (blade), C-reeks (rack) en X-reeks (modulair) platforms — worden geleverd met deze Microsoft 2011-certificaten die vooraf zijn geladen in hun UEFI BIOS-firmware. Wanneer Secure Boot is ingeschakeld, gebruikt het BIOS deze certificaten bij elke opstartcyclus om te valideren:

1. De Windows Server-bootloader (bijvoorbeeld `bootmgfw.efi`) — ondertekend door de Windows Production PCA 2011.
2. UEFI-componenten van derden zoals:
   - Optionele Cisco VIC-ROM's (Virtual Interface Card)
   - UEFI-stuurprogramma's voor opslagcontroller (RAID)
   - Netwerkadapter PXE-opstart-ROM's
   - Alle andere PCIe-apparaatfirmware die tijdens POST is geladen

   Deze zijn meestal ondertekend door de Microsoft UEFI CA 2011.

Wat gebeurt er als er geen actie wordt ondernomen?

Zodra de certificaten verlopen zijn, zijn deze storingsscenario's mogelijk op Cisco UCS-servers:

- Windows Server kan niet worden opgestart — De UEFI-firmware kan de Windows-bootloader niet valideren, waardoor Secure Boot het laden van het besturingssysteem

blokkeert. Dit heeft gevolgen voor Windows Server 2016, 2019, 2022 en 2025.

- UEFI-stuurprogramma's en optie-ROM's worden afgewezen — Hardwarecomponenten die afhankelijk zijn van UEFI-stuurprogramma's die zijn ondertekend met het verlopen certificaat, kunnen niet worden geïnitialiseerd tijdens POST. Dit kan leiden tot verlies van toegang tot RAID-volumes, netwerkconnectiviteit tijdens het opstarten van PXE of andere kritieke hardwarefuncties.
- Systemen vallen in een onveilige toestand — Beheerders kunnen in de verleiding komen om Secure Boot uit te schakelen als een tijdelijke oplossing, waardoor een kritieke laag van beveiliging op firmwareniveau wordt geëlimineerd en het nalevingsbeleid van de organisatie kan worden geschonden (bijvoorbeeld NIST, PCI-DSS, HIPAA).
- Grootschalige operationele onderbreking — In bedrijfsomgevingen met honderden of duizenden UCS-servers kan een gecoördineerde gebeurtenis met een opstartfout leiden tot aanzienlijke downtime in datacenters.

Cisco heeft dit probleem formeel getraceerd onder Cisco bug ID CSCwr45526. Dit gebrek erkent dat:

- UCS server BIOS firmware bevat de verlopen Microsoft 2011 Secure Boot certificaten.
- Een BIOS-update is vereist om de vervangende certificaten (Microsoft 2023-certificaten) te introduceren in de UEFI-sleutelwinkels.
- Zonder herstel lopen UCS-servers waarvoor Secure Boot is ingeschakeld na afloop het risico op opstartfouten.

Oplossing

Om dit probleem aan te pakken is een gecoördineerde, tweeledige aanpak nodig — waarbij zowel de Cisco UCS-firmware (BIOS) als het Microsoft Windows-besturingssysteem worden bijgewerkt. Geen enkele update alleen is voldoende; beide zijden van de Secure Boot-vertrouwensketen moeten worden gemoderniseerd.

1. Cisco UCS BIOS-/firmware-updates toepassen

Bijgewerkte BIOS-firmware voor getroffen UCS-platforms met de nieuwe Microsoft Secure Boot-certificaten:

Nieuw certificaat	Vervangt
Microsoft Windows UEFI CA 2023	Microsoft Windows Production PCA 2011

Nieuw certificaat	Vervangt
Microsoft UEFI CA 2023	Microsoft UEFI CA 2011

Actiestappen:

- Monitor Cisco bug ID CSCwr45526 op de Cisco Bug Search Tool voor vaste firmwareversies en releasetermijnen.
- Download en implementeer het bijgewerkte BIOS wanneer beschikbaar voor uw specifieke UCS-platform (B-reeks, C-reeks, X-reeks).
- Cisco-beheertools gebruiken voor implementatie:
  - Cisco Intersight — Gebruik voor in de cloud beheerde omgevingen het beleid voor firmwarebeheer van Intersight om updates op grote schaal te orkestreren.
  - Cisco UCS Manager (UCSM) — Voor door een domein beheerde servers uit de B-reeks en C-reeks.
  - Cisco IMC (Integrated Management Controller) — voor zelfstandige rackservers uit de C-reeks.

2. Microsoft Windows Updates toepassen

Microsoft is bezig met de uitrol van Secure Boot-certificaatupdates via Windows Update in een gefaseerde aanpak:

fase	Beschrijving	tijdlijn
Fase 1 — Voorbereiding	Nieuwe 2023-certificaten worden toegevoegd aan de Secure Boot db. De oude certificaten uit 2011 blijven betrouwbaar. Oude en nieuwe certificaten bestaan naast elkaar.	Nu beschikbaar
Fase 2 — Overgang	Nieuwe bootmanagers die zijn ondertekend met de 2023-certificaten worden geïmplementeerd. Systemen maken gebruik van de nieuwe vertrouwensketen.	Geleidelijke uitrol (2025-2026)
Fase 3 — Handhaving	Oude certificaten uit 2011 worden toegevoegd aan de DBX (Forbidden Signature Database), waardoor ze effectief worden ingetrokken. Alleen de nieuwe certificaten zijn betrouwbaar.	Na afloop

Actiestappen:

- Zorg ervoor dat op alle UCS-servers waarop Windows Server wordt uitgevoerd de nieuwste cumulatieve updates zijn geïnstalleerd.
- Besteed bijzondere aandacht aan Secure Boot-gerelateerde updates in Microsoft-release notes.
- Sla fase 1- en fase 2-updates niet over - het zijn vereisten voor een soepele overgang.

3. Het milieu valideren

Nadat u zowel firmware- als OS-updates hebt toegepast, valideert u de status Veilig opstarten op elke server:

Van Windows PowerShell:

powershell
Code kopiëren

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

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

Cisco IMC/Intersight:

- Controleer of de BIOS-versie de bijgewerkte firmware weergeeft.
- Bevestigen dat Secure Boot nog steeds is ingeschakeld in het BIOS-beleid.

4. Aanbevolen hersteltijd

tijdsbestek	Actie	Prioriteit
Nu – Q2 2026	Inventariseer alle UCS-servers met Secure Boot ingeschakeld. Abonneer u op updates voor Cisco bug ID CSCwr45526.	Hoog
Q2 – Q3 2026	Test de bijgewerkte BIOS-firmware in een laboratorium-/staging-omgeving. Pas Windows Fase 1- en Fase 2-updates toe.	Hoog
Q3 2026	Begin met de productie van BIOS-updates en Windows-updates in de UCS-vloot.	Hoog
Voor 19 oktober 2026	Alle updates voltooien. Valideer de status Secure Boot op alle servers.	Critical (Kritiek)
na afloop	Monitor voor fase 3 handhaving. Zorg ervoor dat er geen systemen worden gemist.	Gemiddeld

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.