Atténuer l'expiration du certificat Microsoft Secure Boot

Introduction

Ce document décrit comment limiter l'expiration prochaine des certificats d'amorçage sécurisés en ce qui concerne les environnements Cisco UCS.

Informations générales

Secure Boot est une fonction de sécurité fondamentale intégrée à l'interface UEFI (Unified Extensible Firmware Interface) des serveurs et des PC modernes. Il établit une chaîne de confiance pendant le processus de démarrage en s'assurant que seuls les logiciels signés et vérifiés numériquement (chargeurs de démarrage, noyaux de système d'exploitation et pilotes UEFI) sont autorisés à s'exécuter. Ce mécanisme protège les systèmes contre les bootkits, les rootkits et d'autres programmes malveillants de bas niveau.

Au coeur du démarrage sécurisé se trouve un ensemble de certificats cryptographiques émis par Microsoft. Ces certificats sont intégrés dans le micrologiciel UEFI de pratiquement tous les serveurs et ordinateurs livrés au cours de la dernière décennie, y compris les serveurs Cisco UCS (Unified Computing System). Ils servent d'ancres de confiance qui valident la légitimité d'un logiciel d'amorçage.

Microsoft a maintenant révélé que deux certificats d'amorçage sécurisé critiques — le Microsoft Windows Production PCA 2011 et le Microsoft UEFI CA 2011 — expirent le 19 octobre 2026. Cette expiration affecte l'ensemble de l'écosystème matériel et Cisco a reconnu l'impact sur sa gamme de serveurs UCS sous l'ID de bogue Cisco CSCwr45526

Problème

Quels certificats arrivent à expiration ?

Les deux certificats qui sont au centre de ce problème sont :

Certificat	Rôle	Date d'expiration
Microsoft Windows Production PCA 2011	Signe et valide les chargeurs de démarrage Microsoft Windows	19 octobre 2026
Microsoft UEFI CA 2011	Signe et valide les pilotes UEFI tiers, les ROM optionnelles et les chargeurs de démarrage non Windows	19 octobre 2026

Ces certificats sont stockés dans les magasins de clés de démarrage sécurisé du microprogramme UEFI :

- db (Signature Database) — Contient des certificats de confiance utilisés pour vérifier les binaires de démarrage.
- KEK (Key Exchange Key) : autorise les mises à jour de la base de données de signatures.
- PK (Platform Key) : racine de confiance, généralement détenue par le fabricant OEM (par exemple, Cisco).

Pourquoi ce problème se pose-t-il pour les serveurs Cisco UCS ?

Les serveurs Cisco UCS, y compris les plates-formes de série B (lame), de série C (rack) et de série X (modulaire), sont livrés avec ces certificats Microsoft 2011 préchargés dans leur micrologiciel BIOS UEFI. Lorsque le démarrage sécurisé est activé, le BIOS utilise ces certificats à chaque cycle de démarrage pour valider :

1. Le chargeur de démarrage Windows Server (par exemple, `bootmgfw.efi`), signé par Windows Production PCA 2011.
2. Composants UEFI tiers tels que :
   - Mémoires ROM optionnelles de la carte d'interface virtuelle Cisco
   - Pilotes UEFI du contrôleur de stockage (RAID)
   - Mémoires ROM de démarrage PXE de la carte réseau
   - Tout autre micrologiciel de périphérique PCIe chargé pendant le POST

   Ils sont généralement signés par le CA 2011 de l'UEFI de Microsoft.

Que Se Passe-T-Il Si Aucune Action N'Est Entreprise ?

Une fois les certificats expirés, ces scénarios d'échec sont possibles sur les serveurs Cisco UCS :

- Échec du démarrage de Windows Server — Le microprogramme UEFI ne parvient pas à valider le chargeur de démarrage Windows, ce qui empêche le chargement du système d'exploitation par Secure Boot. Cela concerne Windows Server 2016, 2019, 2022 et 2025.
- Les pilotes UEFI et les ROM optionnelles sont rejetés — L'initialisation des composants matériels qui reposent sur des pilotes UEFI signés avec le certificat arrivant à expiration peut échouer pendant le POST. Cela peut entraîner une perte de l'accès aux volumes RAID, de la connectivité réseau lors du démarrage PXE ou d'autres fonctions matérielles critiques.
- Les systèmes ne sont pas sécurisés — Les administrateurs peuvent être tentés de désactiver Secure Boot comme solution de contournement, ce qui élimine une couche critique de sécurité au niveau du micrologiciel et peut enfreindre les politiques de conformité de l'entreprise (par exemple, NIST, PCI-DSS, HIPAA).
- Interruption des opérations à grande échelle — Dans les environnements d'entreprise comptant des centaines ou des milliers de serveurs UCS, une panne de démarrage coordonnée peut entraîner des temps d'arrêt importants dans les data centers.

Cisco a officiellement suivi ce problème sous ID de bogue Cisco CSCwr45526. Ce défaut reconnaît que :

- Le microprogramme BIOS du serveur UCS contient les certificats de démarrage sécurisé Microsoft 2011 qui arrivent à expiration.
- Une mise à jour du BIOS est nécessaire pour introduire les certificats de remplacement (certificats Microsoft 2023) dans les magasins de clés UEFI.
- Sans correction, les serveurs UCS sur lesquels Secure Boot est activé risquent de connaître des échecs de démarrage après expiration.

Solution

La résolution de ce problème nécessite une approche coordonnée sur deux fronts : la mise à jour du micrologiciel Cisco UCS (BIOS) et du système d'exploitation Microsoft Windows. Aucune mise à jour seule n'est suffisante ; Les deux parties de la chaîne de confiance Secure Boot doivent être modernisées.

1. Appliquer les mises à jour du BIOS/micrologiciel Cisco UCS

Mise à jour du micrologiciel du BIOS pour les plates-formes UCS concernées, qui inclut les nouveaux certificats Microsoft Secure Boot :

Nouveau certificat	Remplace
Microsoft Windows UEFI CA 2023	Microsoft Windows Production PCA 2011
Microsoft UEFI CA 2023	Microsoft UEFI CA 2011

Étapes d'action :

- Surveillance du bogue Cisco ID CSCwr45526 sur l'outil de recherche de bogues Cisco pour les versions de microprogramme fixes et les calendriers de publication.
- Téléchargez et déployez le BIOS mis à jour, le cas échéant, pour votre plate-forme UCS spécifique (série B, série C, série X).
- Utilisez les outils de gestion Cisco pour le déploiement :
  - Cisco Intersight : pour les environnements gérés dans le cloud, utilisez les politiques de gestion du micrologiciel Intersight pour orchestrer les mises à jour à grande échelle.
  - Cisco UCS Manager (UCSM) : pour les serveurs gérés par domaine série B et série C.
  - Cisco IMC (Integrated Management Controller) : pour les serveurs rack autonomes série C.

2. Appliquer les mises à jour Microsoft Windows

Microsoft déploie les mises à jour du certificat Secure Boot via Windows Update selon une approche progressive :

Phase	Description	Calendrier
Phase 1 — Préparation	De nouveaux certificats 2023 sont ajoutés à la base de données Secure Boot. Les anciens certificats 2011 restent fiables. Les anciens et les nouveaux certificats coexistent.	Disponible dès maintenant
Phase 2 — Transition	De nouveaux gestionnaires de démarrage signés avec les certificats 2023 sont déployés. Les systèmes commencent à utiliser la nouvelle chaîne de confiance.	Déploiement progressif (2025-2026)
Phase 3 — Application	Les anciens certificats 2011 sont ajoutés à la base de données de signatures interdites (DBX), ce qui les révoque. Seuls les nouveaux certificats sont approuvés.	Post-expiration

Étapes d'action :

- Assurez-vous que les dernières mises à jour cumulées sont installées sur tous les serveurs UCS exécutant Windows Server.
- Soyez particulièrement attentif aux mises à jour relatives au démarrage sécurisé dans les

notes de version de Microsoft.
- Ne sautez pas les mises à jour des phases 1 et 2, car elles sont indispensables à une transition en douceur.

3. Valider l'environnement

Après avoir appliqué les mises à jour du microprogramme et du système d'exploitation, validez l'état Secure Boot sur chaque serveur :

À partir de Windows PowerShell :

powershell
Copier le code

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

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

Dans Cisco IMC/Intersight :

- Vérifiez que la version du BIOS reflète le micrologiciel mis à jour.
- Vérifiez que le démarrage sécurisé est toujours activé dans la stratégie du BIOS.

4. Calendrier de correction recommandé

Délai	Action	Priorité
Maintenant - T2 2026	Inventaire de tous les serveurs UCS avec démarrage sécurisé activé. Abonnez-vous aux mises à jour sur le bogue Cisco ID CSCwr45526.	Élevé
T2 - T3 2026	Testez la mise à jour du micrologiciel du BIOS dans un environnement de travaux pratiques/de préparation. Application des mises à jour de Windows Phase 1 et Phase 2.	Élevé
T3 2026	Commencez le déploiement en production des mises à jour du BIOS et de Windows sur l'ensemble du parc UCS.	Élevé
Avant le 19 octobre 2026	Terminez toutes les mises à jour. Validez l'état Secure Boot sur tous les serveurs.	Critical (critique)

Délai	Action	Priorité
Après Expiration	Surveillez l'application de la Phase 3. Assurez-vous qu'aucun système n'est manqué.	Moyen

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.