Atténuer l'expiration du certificat Microsoft Secure Boot

Table des matières

- Introduction
- Informations générales
- Problème
  - Quels certificats arrivent à expiration ?
  - Pourquoi ce problème se pose-t-il pour les serveurs Cisco UCS ?
  - Que Se Passe-T-Il Si Aucune Action N'Est Entreprise ?
- Solution
  - Application des mises à jour du micrologiciel Cisco UCS
  - Étapes d'action
  - Mode géré Intersight (IMM) - Serveurs
    - Serveurs lames (séries B et X)
    - Serveurs rack (série C) intégrés en mode de gestion intuitif (IMC)
  - Serveurs rack autonomes (série C) - Utilitaire de mise à niveau de l'hôte (HUU)
  - UCS Manager (UCSM) - Serveurs gérés

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 chargeurs de démarrage de logiciels, les noyaux de système d'exploitation et les pilotes UEFI signés et vérifiés numériquement 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 PC 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 les certificats de démarrage sécurisé critiques expirent à partir de juin 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 trois 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	27 juin 2026
Microsoft UEFI CA 2011	Signe et valide les pilotes UEFI tiers, les ROM optionnelles et les chargeurs de démarrage non Windows	27 juin 2026
Microsoft Corporation KEK CA 2011	Signale les mises à jour de DB et DBX.	24 juin 2026

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

- db (Signature Database) — Contient des certificats sécurisés 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 ?

Serveurs Cisco UCS : les plates-formes des gammes B (lame), C (rack) et X (modulaire) sont livrées avec des certificats Microsoft 2011 Secure Boot préchargés dans leur microprogramme BIOS UEFI. Lorsque le démarrage sécurisé est activé, le BIOS utilise ces certificats à chaque

cycle de démarrage pour valider :

- Le chargeur de démarrage du système d'exploitation, signé par l'outil Windows Production PCA 2011.
- Composants UEFI tiers, tels que :
  - Pilotes UEFI du contrôleur de stockage (RAID)
  - Mémoires ROM de démarrage PXE de la carte réseau
  - Autre microprogramme de périphérique PCIe chargé pendant le POST

Ces composants sont généralement signés par la certification Microsoft UEFI CA 2011.

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

- Les systèmes d'exploitation, pilotes et ROM optionnels existants continuent de fonctionner normalement, car ils ont été signés avec les certificats actuellement approuvés et ne dépendent pas de la nouvelle autorité de certification. Par conséquent, les serveurs affectés continuent à démarrer sans interruption. L'expiration affecte seulement les futurs binaires signés avec les nouveaux certificats, elle n'invalide pas rétroactivement les composants déjà signés et déjà approuvés.
- Le point auquel les fichiers sont résignés avec les nouveaux certificats est déterminé par le fournisseur responsable de chaque composant, et non par un seul événement coordonné. Cela s'applique également aux appliances basées sur UCS, où le calendrier est régi par les fournisseurs respectifs et les autorités de signature responsables de ces images.
- Il ne s'agit pas d'un problème spécifique à Windows. Tout système d'exploitation ou composant de microprogramme qui s'appuie sur Secure Boot et adopte les nouveaux certificats de signature est soumis aux mêmes exigences de transition au fil du temps. Pour cette raison, la coordination avec les fournisseurs d'appareils responsables est essentielle. Les conseils publiés par chaque fournisseur et les conseils doivent faire l'objet d'un suivi direct, plutôt que de supposer qu'une seule mise à jour du micrologiciel UCS sous-jacent est suffisante puisque la signature de l'image du système d'exploitation de l'appliance est contrôlée séparément du micrologiciel de la plate-forme.

Ce tableau récapitule le comportement de démarrage attendu en fonction de l'état du certificat CIMC et de l'activation ou non du démarrage sécurisé. Il illustre les cas où une correction (mise à jour de CIMC vers le nouveau certificat) est nécessaire pour préserver la capacité à démarrer les futurs fichiers signés :

État du certificat CIMC	Démarrage sécurisé activé	Démarrage sécurisé activé -	Démarrage sécurisé désactivé	Démarrage sécurisé désactivé
	Fichiers actuels	Futurs fichiers	Fichiers actuels	Futurs fichiers
Ancien CIMC (ancien certificat)	O	X	O	O
Nouveau CIMC (nouveau certificat)	O	O	O	O

Légende : O = Démarrage réussi · X = Échec du démarrage / fichiers non approuvés

Cisco a officiellement suivi ce problème sous l'ID de bogue Cisco CSCwr45526.

Ce défaut reconnaît que :

- Le microprogramme du serveur UCS contient les certificats de démarrage sécurisé Microsoft 2011 qui arrivent à expiration.
- Une mise à jour du micrologiciel est nécessaire pour introduire les certificats de remplacement (certificats Microsoft 2023) dans les magasins de clés UEFI.

Remarque : le problème du certificat Secure Boot ne se produit pas si le serveur UCS s'exécute en mode de démarrage hérité. De même, le mode UEFI avec Secure Boot désactivé n'est pas affecté.

Solution

Application des mises à jour du micrologiciel Cisco UCS

Mise à jour du micrologiciel pour les plates-formes UCS affectées, 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
Microsoft Corporation KEK 2K CA 2023	Microsoft Corporation KEK CA 2011

Étapes d'action

- Surveillez l'ID de bogue Cisco CSCwr4526 sur l'outil de recherche de bogue Cisco pour les versions de microprogramme fixes et les calendriers de publication.
- Téléchargez et déployez le micrologiciel mis à jour, le cas échéant, pour votre plate-forme UCS spécifique (série B, série C, série X).

- Utiliser les outils de gestion Cisco pour la mise à niveau du micrologiciel :
    - 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 des gammes B et C.
    - Cisco IMC (Integrated Management Controller) : pour les serveurs rack autonomes de la gamme C.

Les tableaux suivants contiennent la version minimale du microprogramme qui inclut le correctif avec les certificats mis à jour, les versions supérieures contiennent également le correctif :

Mode géré Intersight (IMM) - Serveurs

Serveurs lames (séries B et X)

Modèle de serveur	Version(s) du micrologiciel
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

Serveurs rack (série C) intégrés en mode de gestion intuitive (IMC)

Version du micrologiciel IMC
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

Version du micrologiciel IMC
IMC-4.3.2.260007

Serveurs rack autonomes (série C) - Utilitaire de mise à niveau de l'hôte (HUU)

Modèle de serveur	Version(s) du micrologiciel
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) - Serveurs gérés

Version du microprogramme UCSM
4.3(6f)
6.0(2b)

Des configurations supplémentaires sont parfois nécessaires pour résoudre le problème d'expiration du certificat UEFI, en fonction du système d'exploitation sur les serveurs UCS. Cisco recommande de contacter le fournisseur du système d'exploitation concerné pour obtenir des conseils sur les étapes de correction spécifiques.



Remarque : Les mises à jour du micrologiciel sur les serveurs UCS ne résolvent pas toujours entièrement le problème. Des mises à jour de certificat au niveau du système d'exploitation peuvent également être nécessaires pour garantir la continuité de la fonctionnalité Secure Boot au-delà de la date d'expiration du certificat UEFI 2026.

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.