Mitigar el vencimiento del certificado de arranque seguro de Microsoft

Introducción

Este documento describe cómo mitigar la próxima expiración de los certificados de arranque seguro en lo que respecta a los entornos Cisco UCS.

Antecedentes

Secure Boot es una función de seguridad básica integrada en la interfaz de firmware extensible unificada (UEFI) de los servidores y PC modernos. Establece una cadena de confianza durante el proceso de arranque al garantizar que solo se permite ejecutar el software firmado y verificado digitalmente (cargadores de arranque, núcleos del sistema operativo y controladores UEFI). Este mecanismo protege los sistemas frente a bootkits, rootkits y otras amenazas de malware de bajo nivel.

En el corazón de Secure Boot se encuentra un conjunto de certificados criptográficos emitidos por Microsoft. Estos certificados están incorporados en el firmware UEFI de prácticamente todos los servidores y PC vendidos en la última década, incluidos los servidores Cisco UCS (Unified Computing System). Sirven como anclajes de confianza que validan si un fragmento de software de arranque es legítimo.

Microsoft ha revelado que dos certificados críticos de arranque seguro, Microsoft Windows Production PCA 2011 y Microsoft UEFI CA 2011, expirarán el 19 de octubre de 2026. Este vencimiento afecta a todo el ecosistema de hardware y Cisco ha reconocido el impacto en su cartera de servidores UCS con la identificación de error de Cisco CSCwr45526

Problema

¿Qué certificados vencen?

Los dos certificados que constituyen el núcleo de esta emisión son:

Certificado	Función	Fecha de vencimiento
Producción PCA 2011 de Microsoft Windows	Firma y valida los cargadores de arranque de Microsoft Windows	19 de octubre de 2026
Microsoft UEFI CA 2011	Firma y valida controladores UEFI de terceros, ROM opcionales y cargadores de inicio que no son de Windows	19 de octubre de 2026

Estos certificados se almacenan en los almacenes de claves de arranque seguro del firmware UEFI:

- db (Signature Database): contiene certificados de confianza utilizados para verificar binarios en tiempo de arranque.
- KEK (clave de intercambio de claves): autoriza las actualizaciones de la base de datos de firmas.
- PK (clave de plataforma): raíz de la confianza, que normalmente pertenece al OEM (por ejemplo, Cisco).

¿Por qué esto supone un problema para los servidores Cisco UCS?

Los servidores Cisco UCS, incluidas las plataformas B-Series (Blade), C-Series (Rack) y X-Series (Modular), se envían con estos certificados de Microsoft 2011 precargados en el firmware del BIOS de UEFI. Cuando se habilita el arranque seguro, el BIOS utiliza estos certificados en cada ciclo de arranque para validar:

1. El cargador de inicio de Windows Server (por ejemplo, `bootmgfw.efi`), firmado por Windows Production PCA 2011.
2. Componentes UEFI de terceros como:
   - ROM opcionales de Cisco VIC (tarjeta de interfaz virtual)
   - Controladores de almacenamiento (RAID) Controladores UEFI
   - ROM de arranque PXE del adaptador de red
   - Cualquier otro firmware de dispositivo PCIe cargado durante la POST

   Estos suelen estar firmados por Microsoft UEFI CA 2011.

¿Qué Ocurre Si No Se Realiza Ninguna Acción?

Una vez caducados los certificados, estos escenarios de fallos son posibles en los servidores Cisco UCS:

- Windows Server no puede arrancar: el firmware UEFI no puede validar el cargador de arranque de Windows, lo que hace que Secure Boot bloquee la carga del SO. Esto afecta a Windows Server 2016, 2019, 2022 y 2025.
- Se rechazan los controladores UEFI y las ROM opcionales: los componentes de hardware que dependen de controladores UEFI firmados con el certificado que caduca pueden no inicializarse durante la POST. Esto podría provocar la pérdida de acceso a los volúmenes RAID, la conectividad de red durante el arranque de PXE u otras funciones de hardware críticas.
- Los sistemas caen en un estado inseguro: los administradores pueden verse tentados a desactivar Secure Boot como solución alternativa, lo que elimina una capa crítica de seguridad de nivel de firmware y puede infringir las políticas de cumplimiento organizativas (por ejemplo, NIST, PCI-DSS, HIPAA).
- Interrupción operativa a gran escala: en entornos empresariales con cientos o miles de servidores UCS, un fallo de arranque coordinado podría provocar un tiempo de inactividad considerable en todos los Data Centers.

Cisco ha realizado un seguimiento formal de este problema en ID de bug de Cisco CSCwr45526 🔍. Este defecto reconoce que:

- El firmware del BIOS del servidor UCS contiene los certificados de inicio seguro de Microsoft 2011 que vencerán.
- Se requiere una actualización del BIOS para introducir los certificados de sustitución (certificados de Microsoft 2023) en los almacenes de claves UEFI.
- Sin la remediación, los servidores UCS con arranque seguro habilitado corren el riesgo de sufrir fallos de arranque tras la expiración.

Solución

Para solucionar este problema se requiere un enfoque coordinado de dos frentes: la actualización del firmware de Cisco UCS (BIOS) y del sistema operativo Microsoft Windows. Ninguna actualización por sí sola es suficiente; ambos lados de la cadena de confianza de arranque seguro deben modernizarse.

1. Aplicar actualizaciones de BIOS/firmware de Cisco UCS

Firmware de BIOS actualizado para las plataformas UCS afectadas que incluye los nuevos certificados de arranque seguro de Microsoft:

Nuevo certificado	Sustituye
UEFI CA 2023 de Microsoft Windows	Producción PCA 2011 de Microsoft Windows
UEFI CA 2023 de Microsoft	Microsoft UEFI CA 2011

Pasos de acción:

- Supervisar ID de bug de Cisco CSCwr45526 en la Herramienta de Búsqueda de Errores de Cisco para versiones fijas de firmware y plazos de lanzamiento.
- Descargue e implemente el BIOS actualizado cuando esté disponible para su plataforma UCS específica (serie B, serie C, serie X).
- Utilice las herramientas de gestión de Cisco para la implementación:
  - Cisco Intersight: para entornos gestionados en la nube, utilice las políticas de gestión de firmware de Intersight para organizar las actualizaciones a escala.
  - Cisco UCS Manager (UCSM): para servidores de la serie B y la serie C gestionados por dominio.
  - Cisco IMC (Integrated Management Controller): para servidores en rack de la serie C independientes.

2. Aplicar actualizaciones de Microsoft Windows

Microsoft está implementando actualizaciones de certificados de arranque seguro a través de Windows Update mediante un enfoque por fases:

Fase	Descripción	Plazos
Fase 1 — Preparación	Se agregan nuevos certificados 2023 a la base de datos de arranque seguro. Los antiguos certificados de 2011 siguen siendo de confianza. Tanto los certificados antiguos como los nuevos coexisten.	Disponible ahora
Fase 2 - Transición	Se implementan nuevos administradores de arranque firmados con los certificados 2023. Los sistemas comienzan a utilizar la nueva cadena de confianza.	Implantación gradual (2025-2026)
Fase 3 — Ejecución	Los certificados antiguos de 2011 se añaden a la DBX (base de datos de firmas prohibidas), revocándolos de forma efectiva. Sólo se confía en los nuevos certificados.	Posterior al vencimiento

Pasos de acción:

- Asegúrese de que todos los servidores UCS que ejecutan Windows Server tienen instaladas las actualizaciones acumulativas más recientes.
- Preste especial atención a las actualizaciones relacionadas con Secure Boot en las notas de la versión de Microsoft.
- No se salte las actualizaciones de las fases 1 y 2, ya que son requisitos previos para una transición fluida.

3. Validar el entorno

Después de aplicar las actualizaciones del firmware y del sistema operativo, valide el estado de arranque seguro en cada servidor:

En Windows PowerShell:

PowerShell
Copiar código

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

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

De Cisco IMC/Intersight:

- Verifique que la versión del BIOS refleje el firmware actualizado.
- Confirmar que el arranque seguro sigue habilitado en la directiva del BIOS.

4. Plazos recomendados para la remediación

Plazo	Acción	Prioridad
Ahora: segundo trimestre de 2026	Realice un inventario de todos los servidores UCS con Secure Boot activado. Suscribirse a actualizaciones sobre el Id. de bug Cisco CSCwr45526 🔍.	Alto
T2 - T3 2026	Pruebe el firmware actualizado del BIOS en un entorno de laboratorio/ensayo. Aplique las actualizaciones de Windows Phase 1 y Phase 2.	Alto
Tercer trimestre de	Comenzar la implementación de producción de actualizaciones de	Alto

Plazo	Acción	Prioridad
2026	BIOS y de Windows en toda la flota de UCS.	
Antes del 19 de octubre de 2026	Complete todas las actualizaciones. Validar el estado de arranque seguro en todos los servidores.	Crítico
Posterior al vencimiento	Supervisar la aplicación de la fase 3. Asegúrese de que no se ha perdido ningún sistema.	Medio

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).