Mitigar Expiração do Certificado de Inicialização Segura da Microsoft

Introdução

Este documento descreve como reduzir a próxima expiração dos certificados de inicialização segura, já que se trata de ambientes Cisco UCS.

Informações de Apoio

A Inicialização Segura é um recurso de segurança básico integrado na Unified Extensible Firmware Interface (UEFI) de servidores e PCs modernos. Estabelece uma cadeia de confiança durante o processo de inicialização, garantindo que somente softwares assinados e verificados digitalmente (carregadores de inicialização, kernels do sistema operacional e drivers UEFI) tenham permissão para execução. Esse mecanismo protege os sistemas contra bootkits, rootkits e outras ameaças de malware de baixo nível.

No centro da Inicialização Segura está um conjunto de certificados criptográficos emitidos pela Microsoft. Esses certificados estão incorporados no firmware da UEFI de praticamente todos os servidores e PCs vendidos na última década, incluindo os servidores Cisco UCS (Unified Computing System). Eles servem como âncoras de confiança que validam se um software de tempo de inicialização é legítimo.

A Microsoft divulgou agora que dois certificados críticos do Secure Boot — o Microsoft Windows Production PCA 2011 e o Microsoft UEFI CA 2011 — estão prestes a expirar em 19 de outubro de 2026. Essa expiração afeta todo o ecossistema de hardware, e a Cisco reconheceu o impacto em seu portfólio de servidores UCS sob a ID de bug Cisco CSCwr45526

Problema

Quais Certificados Estão Expirando?

Os dois certificados no centro desta emissão são:

Certificado	Função	Data de vencimento
APC de produção do Microsoft Windows 2011	Assina e valida carregadores de inicialização do Microsoft Windows	19 de outubro de 2026
Microsoft UEFI CA 2011	Assina e valida drivers UEFI de terceiros, ROMs de opção e carregadores de inicialização não Windows	19 de outubro de 2026

Esses certificados são armazenados no armazenamento de chave de Inicialização Segura do firmware UEFI:

- db (Signature Database) — Contém certificados confiáveis usados para verificar binários de tempo de inicialização.
- KEK (Key Exchange Key) — Autoriza atualizações no Banco de Dados de Assinaturas.
- PK (chave de plataforma) — A raiz da confiança, normalmente de propriedade do OEM (por exemplo, Cisco).

Por que isso é um problema para os servidores Cisco UCS?

Os servidores Cisco UCS, incluindo as plataformas B-Series (Blade), C-Series (Rack) e X-Series (Modular), são fornecidos com esses certificados Microsoft 2011 pré-carregados no firmware do BIOS UEFI. Quando a Inicialização Segura está habilitada, o BIOS usa estes certificados em cada ciclo de inicialização para validar:

1. O carregador de inicialização do Windows Server (por exemplo, `bootmgfw.efi`) — assinado pelo APC de produção do Windows 2011.
2. Componentes UEFI de terceiros como:
   - ROMs opcionais da Cisco VIC (Virtual Interface Card, placa de interface virtual)
   - Drivers UEFI da controladora de armazenamento (RAID)
   - ROMs de inicialização PXE do adaptador de rede
   - Qualquer outro firmware de dispositivo PCIe carregado durante o POST

   Eles são normalmente assinados pela Microsoft UEFI CA 2011.

O Que Acontece Se Nenhuma Ação For Tomada?

Quando os certificados expiram, estes cenários de falha são possíveis nos servidores Cisco UCS:

- Falha na inicialização do Windows Server — O firmware da UEFI não pode validar o carregador de inicialização do Windows, fazendo com que a Inicialização Segura bloqueie o carregamento do sistema operacional. Isso afeta o Windows Server 2016, 2019, 2022 e 2025.
- Os drivers UEFI e as ROMs de opção são rejeitados — Os componentes de hardware que dependem de drivers UEFI assinados com o certificado que está expirando podem não ser inicializados durante o POST. Isso pode resultar em perda de acesso aos volumes RAID, conectividade de rede durante a inicialização PXE ou outras funções críticas de hardware.
- Os sistemas caem em um estado inseguro — Os administradores podem ser tentados a desabilitar a Inicialização Segura como solução alternativa, o que elimina uma camada crítica de segurança em nível de firmware e pode violar as políticas de conformidade organizacional (por exemplo, NIST, PCI-DSS, HIPAA).
- Interrupção operacional em larga escala — Em ambientes corporativos com centenas ou milhares de servidores UCS, um evento coordenado de falha de inicialização pode causar um tempo de inatividade significativo entre data centers.

A Cisco rastreou formalmente esse problema em ID de bug Cisco CSCwr45526. Este defeito reconhece que:

- O firmware do BIOS do servidor UCS contém os certificados do Microsoft 2011 Secure Boot que estão prestes a expirar.
- É necessária uma atualização do BIOS para introduzir os certificados de substituição (certificados Microsoft 2023) nos armazenamentos de chaves da UEFI.
- Sem correção, os servidores UCS com Inicialização Segura habilitada correm o risco de falhas de inicialização após a expiração.

Solução

Para resolver esse problema, é necessária uma abordagem coordenada em duas frentes: atualizar o firmware (BIOS) do Cisco UCS e o sistema operacional Microsoft Windows. Nenhuma atualização isolada é suficiente; os dois lados da cadeia de confiança do Secure Boot devem ser modernizados.

1. Aplicar as atualizações de BIOS/firmware do Cisco UCS

Firmware de BIOS atualizado para as plataformas UCS afetadas que inclui os novos certificados

do Microsoft Secure Boot:

Novo certificado	Substitui
Microsoft Windows UEFI CA 2023	APC de produção do Microsoft Windows 2011
Microsoft UEFI CA 2023	Microsoft UEFI CA 2011

Etapas da ação:

- Monitore o bug da Cisco ID CSCwr45526 na Cisco Bug Search Tool para obter versões de firmware fixas e prazos de lançamento.
- Baixe e implante o BIOS atualizado, quando disponível, para sua plataforma UCS específica (B-Series, C-Series, X-Series).
- Use as ferramentas de gerenciamento da Cisco para implantação:
  - Cisco Intersight — Para ambientes gerenciados em nuvem, use as políticas de gerenciamento de firmware da Intersight para orquestrar atualizações em escala.
  - Cisco UCS Manager (UCSM) — Para servidores gerenciados por domínio B-Series e C-Series.
  - Cisco IMC (Integrated Management Controller, Controlador de gerenciamento integrado) — para servidores rack C-Series autônomos.

2. Aplicar Atualizações do Microsoft Windows

A Microsoft está distribuindo as atualizações do certificado de Inicialização Segura por meio do Windows Update em uma abordagem em fases:

Fase	Descrição	Cronograma
Fase 1 — Preparação	Os novos certificados 2023 são adicionados ao bd do Secure Boot. Os antigos certificados de 2011 permanecem confiáveis. Ambos os certificados antigos e novos coexistem.	Disponível agora
Fase 2 — Transição	Novos gerenciadores de inicialização assinados com os certificados 2023 são implantados. Os sistemas começam a usar a nova cadeia de confiança.	Implantação gradual (2025-2026)
Fase 3 — Aplicação	Os antigos certificados de 2011 são adicionados ao DBX (Forbidden Signature Database), revogando-os efetivamente. Somente os novos certificados são confiáveis.	Pós-expiração

Etapas da ação:

- Verifique se todos os servidores UCS que executam o Windows Server têm as atualizações cumulativas mais recentes instaladas.
- Preste atenção especial às atualizações relacionadas ao Secure Boot nas notas de versão

da Microsoft.
- Não ignore as atualizações das Fases 1 e 2 — elas são pré-requisitos para uma transição tranquila.

3. Validar o Ambiente

Depois de aplicar as atualizações de firmware e de SO, valide o estado Inicialização segura em cada servidor:

Do Windows PowerShell:

powershell
Copiar Código

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

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

Do Cisco IMC/Intersight:

- Verifique se a versão do BIOS reflete o firmware atualizado.
- Confirme se a Inicialização segura ainda está habilitada na política do BIOS.

4. Cronograma de correção recomendado

Cronograma	Ação	Prioridade
Agora - 2º trimestre de 2026	Faça o inventário de todos os servidores UCS com Inicialização Segura habilitada. Assine as atualizações na ID de bug da Cisco CSCwr45526.	Alto
T2 - T3 2026	Testar o firmware atualizado do BIOS em um ambiente de laboratório/preparação. Aplique as atualizações das Fases 1 e 2 do Windows.	Alto
3 o trim. de 2026	Inicie a distribuição da produção de atualizações do BIOS e do Windows pelo conjunto UCS.	Alto
Antes de 19 de outubro de 2026	Conclua todas as atualizações. Valide o estado de Inicialização Segura em todos os servidores.	Crítico

Cronograma	Ação	Prioridade
Pós-expiração	Monitore a aplicação da Fase 3. Verifique se nenhum sistema foi perdido.	Médio

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.