

Aconselhamento de segurança do IOS-XE de correção - agosto de 2026 e problemas críticos relacionados

Contents

Introdução

Este documento descreve os bugs críticos do software sem fio relatados com as versões de segurança reforçada publicadas para o consultivo IOS-XE - agosto de 2026.

Background

Este documento fornece orientação de atualização para abordar o [Security Advisory](#), o [FN74383](#) e os problemas críticos.

Em 5 de agosto de 2026, a Cisco lançou o [IOS-XE Security Hardening Advisory](#) que afeta várias plataformas, incluindo, mas não se limitando a, 9800 Series Wireless LAN Controllers. Conforme documentado, este aviso aborda várias vulnerabilidades descobertas internamente, resultantes de uma análise de segurança interna abrangente pela Engenharia Cisco IOS-XE.

Plataformas sem fio incluídas na revisão

Catalyst Wireless 9800 (C9800-L, C9800-CL, C9800-40, C9800-80)

Cisco Wireless 9800 WLC (CW9800L, CW9800M, CW9800H1/H2)

Wireless 9800 incorporado no switch Catalyst (9800-SW) - suporta apenas a implantação SDA

Pontos de acesso baseados em COS Catalyst 11ax 91xx Series
(9105/9115/9117/9120/9130/9136/9164/9166)

Pontos de acesso Cisco Wireless 917x Series

(CW9171/CW9172/CW9174/CW9176/CW9178/CW9179)

Versão do software Cisco IOS XE	Primeira versão fixa
17.9	17.9.10
17.12	17.12.8
17.15	17.15.6
17.18	17.18.4, 17.18.4a*
26.1	26.1.2

Tabela 1. Versões de software incluídas na revisão e as versões reforçadas correspondentes

 *Nota: 17.18.4a suporta todas as WLCs independentes. Somente para o Wireless Lan Controller incorporado em switches em implantações SDA use o pacote sem fio 17.18.4 que funcionará com a versão do switch 17.18.4. Não haverá uma versão 17.18.4a para switch ou pacote sem fio.

Erros Críticos

Nas versões de segurança reforçada mencionadas na Tabela 1, foram identificados alguns problemas críticos que podem afetar o uso dessas versões.

1. [CSCwv93265](#)
2. [CSCwv98483](#)

Erros Críticos em Detalhes

[CSCwv93265](#)

Sintoma: Falhas de conectividade do cliente ou roaming quando os recursos OpenRoaming, WPA3, 11k, 11v, 11r estão em uso.

Plataformas afetadas: Todos os Cisco 9800 Wireless Controller e Wireless Package para Cat9K.

Versão do software afetado: Cisco IOS XE 26.1.2, Cisco IOS XE 17.18.4a, Cisco IOS XE 17.18.4, Cisco IOS XE 17.15.6, Cisco IOS XE 17.12.8, Cisco IOS XE 17.9.10

Próxima etapa: Um APSP corretivo está disponível para 17.12.8, 17.15.6 e 17.18.4a. O lançamento do APSP corretivo para outras versões do IOS-XE (17.9.10, 26.1.2) está planejado para 15 de agosto. A Cisco recomenda implantar o APSP assim que ele for lançado.

Versão fixa:

	C9800-L	CW9800-L	C9800-40	C9800-80	C9800-CL	CW9800-M	CW9800-H1	CW9800-H2	Switches cat9k	C9350	CER-on-
--	---------	----------	----------	----------	----------	----------	-----------	-----------	----------------	-------	---------

											9100s
17.15.6	APSP-Link	NA	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	NA	Entre em contato com o TAC para obter a versão Especial da Engenharia
17.18.4a	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	NA	NA	NA
17.18.4	NA	NA	NA	NA	NA	NA	NA	NA	APSP-Link	NA	NA
17.12.8	APSP-Link	NA	APSP-Link	APSP-Link	APSP-Link	NA	NA	NA	APSP-Link	NA	Mudar para o trem 17.15
26.1.2	Planejado para 15 de agosto	Planejado para 15 de agosto	Planejado para 15 de agosto	Planejado para 15 de agosto	Planejado para 15 de agosto	Planejado para 15 de agosto	Planejado para 15 de agosto	Planejado para 15 de agosto	Planejado para 15 de agosto	Planejado para 15 de agosto	NA
17.9.10	APSP-Link	NA	APSP-Link	APSP-Link	APSP-Link	NA	NA	NA	APSP-Link	NA	Mudar para o trem 17.15

Tabela 2. Links APSP para diferentes plataformas de WLC 9800

[CSCwv98483](#)

Sintoma: Clientes sem fio ancorados presos no IP_Learn quando o C9800-L, o CW9800-L e o C9800-CL estiverem configurados como WLC externo

Plataformas afetadas: C9800-L, CW9800-L, C9800-CL (somente no cenário Guest-Anchor em que as plataformas afetadas atuam como WLC externas)

Versão do software afetado: Cisco IOS XE 26.1.2, Cisco IOS XE 17.18.4a, Cisco IOS XE 17.15.6

Solução: Ative a criptografia de enlace de dados de mobilidade no túnel entre o exterior e a âncora:

```
wireless mobility group member mac-address <peer_mac> ip <peer_ip> public-ip <peer_ip> group <peer_group>
```

Versão fixa: A Cisco está trabalhando ativamente em um SMU de patch/cold patch fixo e os clientes serão notificados assim que ele se tornar disponível (Versão planejada: 21 de agosto). Este será um SMU frio que requer uma recarga da WLC.

Orientação de atualização para problemas de consultoria e críticos

Para resolver os problemas críticos e de consultoria relatados nas versões de segurança reforçada, a Cisco recomenda

Etapa 1. Os clientes sem fio que executam o IOS-XE versão 17.12, 17.15, 17.18 prosseguem para as Etapas 2, 3 e 4. Os clientes sem fio que executam o IOS-XE versão 17.9, 26.1 aguardam até que o patch APSP seja publicado em cisco.com ANTES da atualização. Consulte a Tabela 2 para obter as datas de lançamento dos patches

Etapa 2. Antes da atualização, execute as verificações de atualização e as etapas de recuperação documentadas [aqui](#) para reduzir o impacto devido ao [FN74383](#)

Etapa 3. Atualize a versão IOS-XE com segurança reforçada e o patch APSP na mesma janela de manutenção para evitar que o serviço sem fio seja afetado.

Etapa 4. Se for afetado pelo [CSCwv98483](#), aplique a solução alternativa até que o SMU esteja disponível. Após a publicação do SMU, espera-se que os clientes apliquem o patch SMU.

Considerações sobre tempo de inatividade para planejamento da janela de manutenção para atualização + patches do IOS-XE

A atualização do IOS-XE em 9800 WLCs configuradas em configurações redundantes não redundantes ou de alta disponibilidade (HA) pode aproveitar vários mecanismos, como

- Atualização de software em serviço (ISSU)
- Atualização contínua N+1
- Atualização única

Para obter detalhes, consulte o [Guia de início rápido de atualização da WLC 9800](#)

Além disso, os problemas críticos exigem a aplicação de patches com a SMU (Software Maintenance Update, atualização de manutenção de software) e o APSP (Access Point Service Pack, pacote de serviços de ponto de acesso)

Para obter detalhes sobre várias opções de patch suportadas pelo 9800 WLC, consulte [Patching and Rolling AP Upgrade Guide for 9800 WLC](#)

Para planejar sua janela de manutenção para a atualização + correção do IOS-XE com cada mecanismo de atualização, leve em conta o tempo de inatividade e o impacto documentados nesta seção.

Atualização de software em serviço (ISSU)

- Aplicável apenas ao par de 9800 WLC em execução na configuração de HA Stateful Switchover (HA SSO) e suportado apenas entre versões de longa duração e suas versões de manutenção. (Não suportado em versões de expansão e versões de vida curta sem versões de manutenção)
- O ISSU oferece uma experiência de atualização contínua, suportando 9800 pares em HA SSO enquanto executa versões de software diferentes e aproveita a atualização de AP deslocável. Em um par HA operacional 9800, a WLC em standby é atualizada e, após o SSO, a nova WLC em standby é atualizada. Para obter detalhes do processo ISSU e as CLIs e instantâneos da GUI correspondentes, consulte [Upgrade 9800 HA SSO using ISSU](#)
- Execute as verificações de atualização e a recuperação nos APs antes de iniciar o ISSU.
- Com o ISSU, a duração da atualização não é facilmente previsível. Dependendo do tamanho da implantação e da velocidade da rede, a atualização pode levar várias "horas" para ser concluída
- Além disso, o ISSU aproveita a atualização contínua de APs onde os APs são reinicializados de forma escalonada para minimizar o tempo de inatividade. No entanto, nesse caso, isso significa que os clientes conectados aos APs que executam a versão reforçada continuarão a ter problemas de conectividade e roaming documentados em [CSCwv93265](#) e [CSCwv98483](#) até que a WLC seja corrigida após o upgrade do ISSU.
- O SMU para [CSCwv98483](#) é um patch frio que exige a recarga da WLC.
- O APSP para [CSCwv93265](#) pode ser aplicado usando a atualização de AP deslocável ou em um único disparo. Se estiver usando a atualização de AP deslocável, dependendo do tamanho da implantação, isso pode levar várias "horas" para todos os APs serem atualizados e definitivamente evitar bugs críticos conhecidos
- **Duração total em que o serviço pode ser afetado (WLC ou APs estão inoperantes OU a conectividade/roaming do cliente é afetada) = Tempo para concluir ISSU + Tempo para recarregamento da WLC devido a correção a frio SMU + Tempo para atualização de AP para APSP**

Atualização de N+1 Rolling AP

- Este procedimento se baseia em uma WLC 9800 sobressalente chamada N+1 WLC com versão de software atualizada para hospedar APs, enquanto o par 9800 de "produção" ou o 9800 autônomo passa por atualização. A recomendação é que essa WLC N+1 9800 não tenha APs registrados ANTES do início da atualização contínua N+1.
- Execute as verificações de upgrade e a recuperação em APs enquanto eles estão registrados na WLC primária
- Para obter detalhes sobre o processo e os instantâneos de CLI e GUI associados, consulte [Upgrade 9800 WLC using N+1 Rolling AP upgrade](#)
- Nesse processo, para que os APs façam o roll-over da WLC primária para a WLC N+1, a versão do software em execução na WLC N+1 e pré-baixada para os APs precisa corresponder exatamente.
- O pré-download para APs é facilitado pelo download, mas NÃO pela ativação da versão reforçada do IOS-XE na WLC primária. Sem a ativação da imagem, os patches de software não podem ser aplicados ou pré-baixados para APs. O que, por sua vez, significa que a

WLC N+1 também não pode ser corrigida.

- Mesmo nesse processo, como o ISSU, os APs transferidos para a WLC N+1 continuarão em risco para problemas de conectividade de cliente e roaming documentados em [CSCwv93265](#) e [CSCwv98483](#) até que a WLC N+1 seja corrigida, após o término da atualização do AP deslocável.
- O SMU para [CSCwv98483](#) é um patch frio que exige a recarga da WLC.
- O APSP para [CSCwv93265](#) pode ser aplicado usando a atualização de AP deslocável ou em um único disparo. Se estiver usando a atualização de AP deslocável, dependendo do tamanho da implantação, isso pode levar várias "horas" para todos os APs serem atualizados e definitivamente evitar bugs críticos conhecidos
- **Duração total em que o serviço pode ser afetado (WLC ou APs estão inoperantes OU a conectividade/roaming do cliente é afetada) = Tempo levado para que todos os APs passem para a WLC N+1 + Tempo para o recarregamento da WLC devido ao patch de SMU frio + Tempo para o upgrade do AP para APSP**
- Para sua janela de manutenção, leve também em conta o tempo levado para que a WLC N+1 seja atualizada para as versões fortalecidas do IOS-XE e para que os APs façam o pré-download da versão fortalecida do IOS-XE a partir da WLC primária, embora nenhum deles tenha qualquer impacto no serviço

Atualização de AP regular N+1 - RECOMENDADO

- Este procedimento se baseia em chamadas de WLC 9800 sobressalentes como N+1 WLC com versão de software atualizada para hospedar APs, enquanto a "produção" do par 9800 ou 9800 autônomo passa por atualização.
- A recomendação é que esse WLC 9800 sobressalente não tenha APs registrados ANTES do início da atualização contínua N+1.
- A WLC N+1 sobressalente pode ser atualizada para IOS-XE reforçado ativado e comprometido e corrigido com APSP e SMU, em uma única tentativa. Sem APs registrados, esse é um impacto fora do serviço, mas você deve considerar o tempo gasto para o recarregamento de várias WLCs ao agendar sua janela de manutenção
- Na GUI da WLC principal onde os APs são registrados, navegue para Configuração > Tags e perfis: Purgamento de AP > Base Primária
 - Definir WLC N+1 e endereço IP da interface de gerenciamento sem fio (WMI) como primário
 - Definir o nome da WLC primária atual e o IP da WMI em Secundário
- Use filtros regex para migrar APs em massa da WLC primária para a WLC N+1.
- Depois de registrados na WLC N+1, os APs já estarão executando a versão de segurança reforçada junto com patches para corrigir bugs críticos.

Duração total em que o serviço pode ser afetado (WLC ou APs estão inativos OU a conectividade/roaming do cliente é afetada) = Tempo levado para que os APs migrem da WLC primária para a WLC N+1, que é ditado pela velocidade da rede entre AP e WLCs.

Atualização única - RECOMENDADO, se não houver WLC N+1

- Neste procedimento, a WLC primária é atualizada (juntamente com ativação e

comprometimento) para a versão IOS-XE com segurança reforçada em uma etapa.

- Como parte da ativação da imagem, a WLC primária é recarregada e todos os APs são registrados novamente na WLC primária de atualização e recebem a versão IOS-XE de segurança reforçada.
- Até que o APSP seja aplicado, os APs estarão em risco para problemas de conectividade e roaming de clientes documentados em [CSCwv93265](#) e [CSCwv98483](#)

Duração total em que o serviço pode ser afetado (WLC ou APs estão inativos OU a conectividade/roaming do cliente é afetada) = Tempo levado para a WLC primária recarregar + Tempo levado para todos os APs baixarem a versão do IOS-XE fortalecido da WLC primária sobre CAPWAP e registrarem de volta na WLC primária. (Dobre esse tempo se o patch SMU estiver sendo aplicado) + Tempo levado para todos os APs baixarem o patch APSP da WLC primária e registrarem de volta na WLC primária.

Perguntas mais freqüentes

P1. Os APs são afetados por este Security Advisory?

Os pontos de acesso baseados em COS foram incluídos na revisão de segurança e as correções correspondentes são incorporadas nas versões IOS-XE reforçadas

Q2. Qual é o risco para WLCs AireOS?

As WLCs AireOS não foram incluídas na revisão de segurança, pois alcançaram o último dia de suporte (LDoS)

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.