

Remediar el aviso de seguridad de IOS-XE: agosto de 2026 y los problemas críticos relacionados

Contenido

Introducción

Este documento describe los errores críticos de software inalámbrico notificados con las versiones de seguridad reforzada publicadas para el aviso de IOS-XE - Agosto de 2026.

Background

Este documento proporciona una guía de actualización para abordar el [Security Advisory, FN74383](#) y los problemas críticos.

El 5 de agosto de 2026, Cisco publicó el [consejo de refuerzo de la seguridad IOS-XE](#) que afecta a varias plataformas, incluidos, entre otros, los controladores de LAN inalámbrica de la serie 9800. Como se ha documentado, este aviso aborda varias vulnerabilidades descubiertas internamente como resultado de una revisión de seguridad interna completa realizada por el departamento de ingeniería de Cisco IOS-XE.

Plataformas inalámbricas incluidas en la revisión

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

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

Red inalámbrica integrada 9800 en switch Catalyst (9800-SW): solo admite la implementación de SDA

Puntos de acceso Catalyst 11ax 91xx Series basados en COS
(9105/9115/9117/9120/9130/9136/9164/9166)

Puntos de acceso inalámbricos de Cisco serie 917x (CW9171/CW9172/CW9174/CW9176/CW9178/CW9179)

Versión del software Cisco IOS XE	Primera versión fija
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

Tabla 1. Versiones de software incluidas en la revisión y las correspondientes versiones reforzadas

 * Nota: 17.18.4a soporta todos los WLC independientes. Solo para el controlador de LAN inalámbrica integrado en switches en implementaciones SDA, utilice el paquete inalámbrico 17.18.4 que funcionará con la versión de switch 17.18.4. No habrá una versión 17.18.4a para el paquete de switch o inalámbrico.

Errores críticos

En las versiones reforzadas de seguridad mencionadas en la tabla 1, se han identificado algunos problemas importantes que pueden afectar al uso de estas versiones.

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

Errores críticos en detalle

[CSCwv93265](#)

Síntoma: Errores de conectividad de cliente o itinerancia cuando se están utilizando las funciones de OpenRoaming, WPA3, 11k, 11v, 11r.

Plataformas afectadas: Todo el controlador inalámbrico Cisco 9800 y el paquete inalámbrico para Cat9K.

Versión de software afectada: 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 y Cisco IOS XE 17.9.10

Siguiente paso: Hay disponible un APSP correctivo para 17.12.8, 17.15.6 y 17.18.4a. Está previsto que el 15 de agosto se publique el APSP correctivo para otras versiones de IOS XE (17.9.10, 26.1.2). Cisco recomienda implementar APSP una vez que se libere APSP.

Versión fija:

	C980-L	CW9800-L	C9800-40	C9800-80	C9800-CL	CW9800-M	CW9800-H1	CW9800-H2	Switches cat9k	C9350	EWC-on-9100
17.15.6	APSP-Link	NA	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	NA	Póngase en contacto con el TAC para obtener la construcción especial de ingeniería
17.18.4 bis	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	Mover a 17.15 tren
26.1.2	Previsto para el 15 de agosto	Previsto para el 15 de agosto	Previsto para el 15 de agosto	Previsto para el 15 de agosto	Previsto para el 15 de agosto	Previsto para el 15 de agosto	Previsto para el 15 de agosto	Previsto para el 15 de agosto	Previsto para el 15 de agosto	Previsto para el 15 de agosto	NA
17.9.10	APSP-Link	NA	APSP-Link	APSP-Link	APSP-Link	NA	NA	NA	APSP-Link	NA	Mover a 17.15 tren

Tabla 2. Enlaces APSP para diferentes plataformas WLC 9800

[CSCwv98483](#)

Síntoma: Clientes inalámbricos anclados atascados en IP_Learn cuando C9800-L, CW9800-L, C9800-CL están configurados como WLC externo

Plataformas afectadas: C9800-L, CW9800-L, C9800-CL (solo en el escenario Guest-Anchor en el que las plataformas afectadas actúan como WLC externo)

Versión de software afectada: Cisco IOS XE 26.1.2, Cisco IOS XE 17.18.4a y Cisco IOS XE 17.15.6

Solución alternativa: Habilite el cifrado de link de datos de movilidad en el túnel entre el extranjero y el anclaje:

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

Versión fija: Cisco está trabajando activamente en una SMU con parche/frío fijo y se notificará a los clientes tan pronto como esté disponible (versión prevista: 21 de agosto). Esto será una SMU fría que requiere una recarga del WLC.

Guía de actualización para cuestiones críticas y de asesoramiento

Para abordar los problemas críticos y de asesoramiento de las versiones reforzadas de seguridad, Cisco recomienda

Paso 1. Los clientes de redes inalámbricas que ejecutan la versión 17.12, 17.15, 17.18 de IOS-XE avanzan a los pasos 2, 3 y 4. Los clientes de redes inalámbricas que ejecutan la versión 17.9, 26.1 de IOS-XE, esperan a que el parche de APSP se publique en cisco.com ANTES de actualizar. Consulte la Tabla 2 para conocer las fechas de lanzamiento de los parches

Paso 2. Antes de la actualización, ejecute las comprobaciones de actualización y los pasos de recuperación documentados [aquí](#) para mitigar el impacto debido a [FN74383](#)

Paso 3. Actualice la versión IOS-XE reforzada con seguridad y el parche APSP en la misma ventana de mantenimiento para evitar que el servicio inalámbrico se vea afectado.

Paso 4. Si se ve afectado por [CSCwv98483](#), aplique la solución alternativa hasta que SMU esté disponible. Una vez que SMU se publique, se espera que los clientes apliquen el parche SMU.

Consideraciones sobre el tiempo de inactividad para planificar la ventana de mantenimiento para la actualización IOS-XE + parches

La actualización IOS-XE en WLC 9800 configurados en configuraciones redundantes no redundantes o de alta disponibilidad (HA) puede aprovechar diversos mecanismos como

- In-Service Software Upgrade (ISSU)
- Actualización sucesiva N+1
- Actualización instantánea

Para obtener más detalles, consulte la [Guía de inicio rápido de actualización de 9800 WLC](#)

Además, los problemas críticos requieren la aplicación de parches con la actualización de mantenimiento de software (SMU) y el Service Pack de punto de acceso (APSP)

Para obtener detalles sobre las diversas opciones de parches soportadas por el WLC 9800, consulte la [Guía de Actualización de Parches y Rolling AP para el WLC 9800](#)

Para planificar su ventana de mantenimiento para la actualización IOS-XE + la aplicación de parches con cada uno de los mecanismos de actualización, tenga en cuenta el tiempo de

inactividad y el impacto documentados en esta sección.

In-Service Software Upgrade (ISSU)

- Aplicable únicamente a un par de WLC 9800 que se ejecuta en una configuración de conmutación stateful HA (HA SSO) y solo compatible entre trenes de versiones de larga duración y sus versiones de mantenimiento. (No es compatible con versiones de escalada y trenes de versiones de corta duración sin versiones de mantenimiento)
- ISSU proporciona una experiencia de actualización perfecta al admitir el par 9800 en HA SSO mientras se ejecutan diferentes versiones de software y se aprovecha la actualización de AP sucesiva. En un par operativo 9800 HA, el WLC en espera se actualiza, y el WLC en espera se actualiza después del SSO, nuevo WLC en espera. Para obtener detalles del proceso ISSU y las CLI y las instantáneas de GUI correspondientes, consulte [Actualización de SSO 9800 HA mediante ISSU](#)
- Ejecute las comprobaciones de actualización y la recuperación en los AP antes de iniciar ISSU.
- Con ISSU, la duración de la actualización no es fácilmente predecible. En función del tamaño de la implementación y de las velocidades de la red, la actualización puede tardar varias "horas" en completarse
- Además, ISSU aprovecha la actualización de AP sucesiva donde los AP se reinician de manera escalonada para minimizar el tiempo de inactividad. Sin embargo, en este caso, significa que los clientes conectados a los AP que ejecutan la versión reforzada seguirán experimentando problemas de conectividad y roaming documentados en [CSCwv93265](#) y [CSCwv98483](#) hasta que el WLC sea parcheado después de la actualización de ISSU.
- SMU para [CSCwv98483](#) es un parche en frío que requiere la recarga del WLC.
- APSP para [CSCwv93265](#) se puede aplicar usando la actualización de Rolling AP o en un solo tiro. Si utiliza la actualización de AP Rolling, dependiendo del tamaño de la implementación, esto puede tomar varias "horas" para que todos los AP se actualicen y definitivamente evitar errores críticos conocidos
- Duración total en la que el servicio podría verse afectado (el WLC o los AP están inactivos O la conectividad/itinerancia del cliente se ve afectada) = Tiempo para completar ISSU + Tiempo para la recarga del WLC debido al parche en frío de SMU + Tiempo para la actualización sucesiva del AP para APSP

Actualización de punto de acceso rodante N+1

- Este procedimiento se basa en un WLC 9800 de repuesto llamado N+1 WLC con versión de software actualizada para alojar AP mientras que el par 9800 de "producción" o el WLC 9800 independiente se someten a la actualización. Se recomienda que este WLC N+1 9800 no tenga ningún AP registrado ANTES de que se inicie la actualización sucesiva N+1.
- Ejecute las comprobaciones de actualización y la recuperación en los AP mientras están registrados en el WLC primario
- Para obtener detalles sobre el proceso y las instantáneas CLI y GUI asociadas, refiérase a [Upgrade 9800 WLC using N+1 Rolling AP upgrade](#)
- En este proceso, para que los AP se trasladen sin problemas del WLC primario al WLC N+1,

la versión del software que se ejecuta en el WLC N+1 y predescargado a los AP necesita coincidir exactamente.

- La predescarga a los AP se facilita descargando, pero NO activando la versión endurecida de IOS-XE en el WLC primario. Sin la activación de la imagen, los parches de software no se pueden aplicar o predescargar a los AP. Lo que, a su vez, significa que el WLC N+1 no puede ser parcheado también.
- Incluso en este proceso, al igual que ISSU, los APs transferidos al WLC N+1 seguirán estando en riesgo por problemas de roaming y conectividad del cliente documentados en [CSCwv93265](#) y [CSCwv98483](#) hasta que se aplique un parche al WLC N+1, después de que finalice la actualización del AP rotatorio.
- SMU para [CSCwv98483](#) es un parche en frío que requiere la recarga del WLC.
- APSP para [CSCwv93265](#) se puede aplicar usando la actualización de Rolling AP o en un solo tiro. Si utiliza la actualización de AP Rolling, dependiendo del tamaño de la implementación, esto puede tomar varias "horas" para que todos los AP se actualicen y definitivamente evitar errores críticos conocidos
- Duración total en la que el servicio podría verse afectado (el WLC o los AP están inactivos O la conectividad/itinerancia del cliente se ve afectada) = Tiempo que tardan todos los AP en pasar al WLC N+1 + Tiempo para la recarga del WLC debido al parche en frío de SMU + Tiempo para la actualización rotatoria del AP para el APSP
- Para su ventana de mantenimiento, también tenga en cuenta el tiempo empleado para que el WLC N+1 se actualice a las versiones reforzadas de IOS-XE y para que los AP predescarguen la versión reforzada de IOS-XE del WLC primario, aunque ninguna de estas dos opciones tendrá ningún impacto en el servicio

Actualización de AP regular N+1 - RECOMENDADO

- Este procedimiento se basa en un WLC 9800 de repuesto como WLC N+1 con versión de software actualizada para alojar AP mientras que el par 9800 de "producción" o el independiente 9800 se somete a la actualización.
- La recomendación es que este WLC 9800 de repuesto no tenga ningún AP registrado para él ANTES de que se inicie la actualización sucesiva N+1.
- El WLC N+1 de repuesto se puede actualizar a IOS-XE reforzado activado y confirmado, y se le puede aplicar un parche con APSP y SMU, en una sola toma. Al no haber ningún AP registrado, esto no afecta al servicio, pero debe tener en cuenta el tiempo que se tarda en la recarga de WLC múltiple al programar su ventana de mantenimiento
- En la GUI principal del WLC donde se registran los AP, navegue hasta Configuración > Etiquetas y perfiles: Primación de PA > Base principal
 - Defina el WLC N+1 y la dirección IP de la interfaz de administración inalámbrica (WMI) como principal
 - Defina el nombre WLC principal actual y la IP WMI en Secundario
- Utilice filtros regex para migrar de forma masiva los AP del WLC principal al WLC N+1.
- Una vez registrados en el WLC N+1, los AP ya estarán ejecutando la versión reforzada de la seguridad junto con los parches para fijar los bugs críticos.

Duración total en la que el servicio podría verse afectado (el WLC o los AP están inactivos O la conectividad/itinerancia del cliente se ve afectada) = Tiempo que los AP tardan en migrar del WLC principal al WLC N+1 que es dictado por la

velocidad de la red entre el AP y los WLC.

Actualización One-Shot - RECOMENDADA, si no hay ningún WLC N+1 presente

- En este procedimiento, el WLC primario se actualiza (junto con la activación y el compromiso) a la versión IOS-XE reforzada de la seguridad en un paso.
- Como parte de la activación de la imagen, el WLC primario se recarga y todos los AP se registrarán de nuevo con el WLC primario del upgrade y recibirán la versión IOS-XE reforzada de la seguridad.
- Hasta que se aplique el APSP, los AP estarán en riesgo por problemas de conectividad e itinerancia del cliente documentados en [CSCwv93265](#) y [CSCwv98483](#)

Duración total en la que el servicio podría verse afectado (el WLC o los AP están inactivos O la conectividad/itinerancia del cliente se ve afectada) = Tiempo que tarda el WLC primario en recargarse + Tiempo que tardan todos los AP en descargar la versión IOS-XE reforzada del WLC primario sobre CAPWAP y en registrarse nuevamente en el WLC primario. (Doble este tiempo si se aplica el parche SMU) + Tiempo que tardan todos los AP en descargar el parche APSP del WLC primario y en registrarse nuevamente en el WLC primario.

Preguntas Frecuentes

P1. ¿Los AP se ven afectados por este aviso de seguridad?

Los puntos de acceso basados en COS se incluyeron en la revisión de seguridad y las correcciones correspondientes se incorporan en las versiones reforzadas de IOS-XE

P2. ¿Cuál es el riesgo para los WLC de AireOS?

Los WLC de AireOS no se incluyeron en la revisión de seguridad ya que han alcanzado el Día final de soporte técnico (LDoS)

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).