

Remediate Catalyst SD-WAN Security Advisory: septiembre de 2026

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Flujo de trabajo de remediación](#)

[Paso 1: Recopilar archivos técnicos de administración de todos los gerentes](#)

[Alternativa: Verificación manual \(solo si Admin-Tech no puede ser recolectada\)](#)

[Paso 2: Actualización a una versión de software fija](#)

[Paso 3: Abra un caso TAC y cargue archivos técnicos de administración para escanear](#)

[Paso 4: Si se identifica un riesgo: guía del TAC](#)

[Versiones de software fijas](#)

[Apéndice: Pasos de verificación manual \(solo si no es posible la recopilación de tecnología de administrador\)](#)

[Cómo identificar los indicadores de compromiso](#)

[Verificación 1: Auditar el registro de acceso del proxy de servicio](#)

[Verificación 2: Auditar el registro de Manager Server](#)

[Preguntas Frecuentes](#)

Introducción

Este documento describe los pasos para identificar y solucionar una vulnerabilidad de seguridad crítica de la SD-WAN según las fechas de asesoramiento de PSIRT del 30 de septiembre de 2026. Cisco recomienda encarecidamente actualizar a una versión de software fija para solucionar este problema.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Componentes de control y arquitectura SD-WAN de Cisco Catalyst (administrador, controlador y validador)
- Procedimiento de actualización de Cisco Catalyst SD-WAN

- Administración de casos del TAC de Cisco y procedimientos de recopilación de tecnología de administración

Componentes Utilizados

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Para obtener información general detallada y las últimas actualizaciones, consulte la página oficial de asesoramiento sobre PSIRT.

Este aviso está disponible en este enlace:

- [Vulnerabilidad de omisión de autenticación API de Cisco Catalyst SD-WAN Manager](#) (CVE-2026-76504, CWE-177). Índice de impacto en la seguridad: Crítico (puntuación base de CVSS 9,8).

Este defecto se aborda en este aviso de PSIRT:

- ID de bug de Cisco [CSCww79570](#)

Este aviso afecta a Cisco Catalyst SD-WAN Manager (vManage).

Flujo de trabajo de remediación



Nota: Todos los administradores de SD-WAN (vManage) que ejecutan una versión anterior a la primera versión fija son vulnerables y requieren una actualización inmediata. Sin embargo, no todos los administradores de Catalyst muestran evidencia de compromiso.

Acción requerida: Recopile técnicos de administración de todos los Catalyst SD-WAN Managers, actualice todos a una versión fija y abra un caso de Cisco TAC para que TAC pueda analizar sus técnicos de administración en busca de indicadores de compromiso.

TAC está disponible para:

- Analice los técnicos de administración que proporcione para ver los indicadores de compromiso
- Proporcionar soporte de actualización si experimenta problemas durante la actualización

- Guiarle a través de soluciones adicionales si se identifican indicadores de compromiso.
1. Recopile Admin-Techs - Ejecute admin-tech en todos los Catalyst SD-WAN Managers, incluyendo cada nodo de un cluster y de una implementación de Recuperación ante Desastres (DR), antes de la actualización para asegurarse de que no se pierdan datos de diagnóstico. Seleccione las opciones Log (Registro) y Tech (Tecnología). El núcleo no es necesario.
 2. Actualizar a una versión fija: actualice todos los jefes (vManage) a una versión de software fija enumerada en la tabla [Versiones de software fijas](#).
-



Nota: No espere los resultados del análisis del TAC antes de actualizar. La actualización a una versión fija es la prioridad más alta y cierra la vulnerabilidad. El análisis del TAC del paso 3 determina si se necesita alguna acción adicional después de la actualización.

3. Abra un caso del TAC y cargue los técnicos de administración para buscar indicadores de compromiso - Abra un caso del TAC de Cisco y cargue todos los paquetes de registro de la tecnología de administración recopilados en el paso 1. El TAC escanea los técnicos de administración en busca de indicadores de compromiso.
 4. Si se identifica un riesgo, utilice la guía del TAC: si el TAC identifica indicadores de riesgo en su entorno, complete toda la guía de remediación proporcionada por el TAC. Si no se encuentran indicadores de compromiso, no se requiere ninguna acción adicional más allá de la actualización.
-

Paso 1: Recopilar archivos técnicos de administración de todos los gerentes

required (obligatorio): Recopile los archivos de administración y tecnología de todos los jefes (vManage) antes de realizar la actualización para asegurarse de que no se pierden datos de diagnóstico. El TAC utiliza estos archivos en el paso 3 para analizar su entorno en busca de indicadores de compromiso.

Colección:



Nota: Para admin-tech generation, seleccione Log and Tech options (Opciones de registro y tecnología). El núcleo no es necesario.

1. Ejecute admin-tech en ALL Managers (vManage).
2. Si sus jefes se ejecutan como un clúster, ejecute admin-tech en cada miembro del clúster.
3. Si tiene una implementación de recuperación ante desastres (DR), ejecute admin-tech en cada administrador, tanto en el sitio principal como en el sitio DR.



Nota: TAC analiza estos archivos para evaluar su entorno en busca de indicadores de compromiso y guiar la ruta de remediación adecuada.

Alternativa: Verificación manual (solo si Admin-Tech no puede ser recolectada)

Para aquellos que no pueden compartir archivos de administración y tecnología, hay disponibles pasos de verificación manual. Estos pasos proporcionan indicadores preliminares que deben documentarse y compartirse con el TAC.

Consulte la sección [Pasos de Verificación Manual](#) al final de este documento para ver los procedimientos detallados. Documente todas las conclusiones y proporciónelas al TAC en su caso de soporte.

Paso 2: Actualización a una versión de software fija

Después de recopilar los técnicos de administración en el paso 1, actualice todos los administradores (vManage) a una versión de software fija.



Importante: No espere los resultados del análisis del TAC antes de actualizar. La actualización a una versión fija es la prioridad más alta y cierra la vulnerabilidad. El análisis del TAC del paso 3 determina si se necesita alguna acción adicional después de la actualización.

Seleccione la versión adecuada de la tabla [Versiones fijas de software](#) de este documento.



Advertencia: La actualización debe permanecer dentro de su versión principal actual. No actualice a una versión principal superior sin una guía explícita del TAC.

[Actualización de controladores SD-WAN con el uso de vManage GUI o CLI](#)



Nota: Si encuentra algún problema durante la actualización, abra un caso del TAC para obtener soporte para la actualización.

Paso 3: Abra un caso TAC y cargue archivos técnicos de administración para escanear

Después de actualizar en el paso 2, abra un caso de soporte del TAC de Cisco y cargue los archivos admin-tech recopilados en el paso 1. El TAC explora los admin-tech en busca de indicadores de compromiso.

Acciones necesarias:

1. Abra un caso TAC de Gravedad 3 con el CVE-ID "CVE-2026-76504" en el título para iniciar el proceso de escaneo.
2. Cargue TODOS los paquetes de registro de tecnología de administración recopilados en el paso 1 (todos los administradores, incluidos los nodos de clúster y DR).
3. Espere a que el TAC complete el análisis y comunique los resultados.



Nota: El TAC analiza los archivos técnicos de administración y comunica los resultados del análisis. Si no se encuentran indicadores de compromiso, no se requiere ninguna acción adicional más allá de la actualización.

Paso 4: Si se identifica un riesgo: guía del TAC

Si el TAC identifica indicadores de compromiso en su entorno, el TAC se pone en contacto con usted para ofrecerle una guía de remediación específica. Complete todas las instrucciones proporcionadas por el TAC.

Si no se identifican indicadores de compromiso, la actualización realizada en el paso 2 es suficiente y no se requiere ninguna otra solución.

Versiones de software fijas

Estas versiones de software contienen la solución para esta vulnerabilidad. Actualice a la primera versión fija de su serie de versiones actual.

Versión del software Cisco Catalyst SD-WAN	Primera versión fija	Software disponible
Anterior a 20.9 ¹	Migrar a una versión fija.	
20.9	20.9.10.1	20.9.10.1 imágenes de actualización para vManage

Versión del software Cisco Catalyst SD-WAN	Primera versión fija	Software disponible
20.12	20.12.8.2	20.12.8.2 imágenes de actualización para vManage
20.15	20.15.6.1	20.15.6.1 imágenes de actualización para vManage
20.18	20.18.4.1	20.18.4.1 imágenes de actualización para vManage
26.1	26.1.2.1	26.1.2.1 imágenes de actualización para vManage
26.2	26.2.1	26.2.1 imágenes de actualización para vManage

¹ Estas versiones han llegado al final del mantenimiento del software. Cisco recomienda encarecidamente a los clientes que actualicen a una versión compatible.

El equipo de respuesta ante incidentes de seguridad de productos (PSIRT) de Cisco valida solo la información de la versión afectada y fija que se documenta en el aviso.



Nota: Cisco también ha solucionado esta vulnerabilidad en Cisco SD-WAN Cloud (Cisco Managed) Release 20.15.605, que está basado en la nube. No se requiere ninguna acción del usuario. Los clientes pueden determinar el estado actual de la solución o la versión del software mediante la función Ayuda de la GUI del servicio.

Referencias importantes:

- [Matriz de actualización](#)
- [Matriz de compatibilidad del controlador](#)

Apéndice: Pasos de verificación manual (solo si no es posible la recopilación de tecnología de administrador)



Nota: La colección Admin-tech es el método preferido y recomendado. Utilice la verificación manual únicamente si no puede recopilar y compartir archivos de tecnología administrativa. Si no puede recopilar archivos de administración-tecnología, utilice estos pasos manuales para recopilar indicadores preliminares para TAC.



Nota:

- Estos pasos proporcionan solo datos preliminares
- La recopilación de tecnología de administración es muy preferible para realizar una evaluación precisa
- Documentar sus conclusiones y compartirlas con el TAC en su caso de soporte
- TAC realiza la determinación de evaluación oficial

Requerimientos: Estos pasos se deben realizar en todos los administradores (vManage), incluidos todos los miembros del clúster y todos los administradores de un sitio de recuperación ante desastres (DR). Acceda a los archivos de registro desde vshell (vshe11 desde la CLI del administrador) y revise tanto los archivos de registro actuales como los rotados.

Cómo identificar los indicadores de compromiso

Esta asesoría tiene dos indicadores de compromiso. Ambas se relacionan con entradas para `j_security_check` en las que un carácter de la solicitud está codificado (por ejemplo, `/%6a_security_check`), desde direcciones IP desconocidas o no autorizadas.



Importante: Los ejemplos de esta sección muestran el uso de `%6a` como el carácter codificado `j` en la solicitud. Esto es sólo un ejemplo, y la vulnerabilidad permite que se utilice cualquier carácter codificado en la solicitud.



Nota: Los sistemas Cisco Catalyst SD-WAN Manager que están expuestos a Internet y que tienen puertos expuestos a Internet corren el riesgo de verse expuestos a peligros. En algunos casos, estos indicadores de compromiso pueden aparecer durante las operaciones estándar. Por lo tanto, deben evaluarse en función del estado normal de la red para identificar y evitar falsos positivos.

Indicador	Archivo de registro	Qué significa	Verificac
Solicitud de <code>j_security_check</code> codificada recibida	<code>/var/log/nms/containers/service_proxy/serviceproxy-access.log*</code>	Un cliente envió una solicitud de este tipo al jefe.	Verificac 1
Solicitud <code>j_security_check</code> codificada procesada para	<code>/var/log/nms/vmanage-server.log*</code>	El administrador ha procesado	Verificac 2

Indicador	Archivo de registro	Qué significa	Verificación
un usuario viptela- reserved-*		una solicitud de este tipo para un usuario viptela-reserved-* (una cuenta de servicio del sistema reservada).	

Verificación 1: Auditar el registro de acceso del proxy de servicio

Audite el archivo `serviceproxy-access.log`, ubicado en `/var/log/nms/containers/service_proxy/serviceproxy-access.log`, en busca de entradas relacionadas con `j_security_check` de direcciones IP desconocidas o no autorizadas, como se muestra en este ejemplo:

```
[2026-09-29T23:11:13.948-05:00] "POST /%6a_security_check HTTP/1.1" 200 - 48 0 4 - "10.10.10.47,192.168
```

Ciertos archivos de registro del sistema vManage están restringidos detrás del acceso raíz y los clientes no pueden acceder directamente a ellos. Para revisar estos registros, los clientes deben generar un archivo `admin-tech`.

Interpretar resultados y documentos para TAC

Si no se encuentra ninguna de estas entradas:

- No se detectaron indicadores de compromiso en este registro de este administrador
- Documente este resultado para su caso TAC
- Continúe con la verificación 2 y, a continuación, repita ambas comprobaciones en los demás jefes

Si se encuentran estas entradas:

- Examine cuidadosamente cada dirección IP de origen mostrada
- Busque entradas de direcciones IP desconocidas o no autorizadas. Verifique si la IP de origen pertenece a una actividad autorizada en su entorno (por ejemplo, un análisis de vulnerabilidad o una prueba de penetración que ejecute)
- Si no puede identificar la IP de origen como legítima, esto puede indicar posibles indicadores de compromiso
- Documentar todas las conclusiones y abrir un caso TAC inmediatamente
- Incluya las entradas del registro, las marcas de tiempo, las IP de origen y los códigos de estado HTTP en su caso

- TAC realiza la determinación de evaluación oficial

Verificación 2: Auditar el registro de Manager Server

Audite el archivo `vmanage-server.log`, ubicado en `/var/log/nms/vmanage-server.log`, en busca de entradas relacionadas con `j_security_check` de direcciones IP desconocidas o no autorizadas, específicamente cuando se llame a usuarios que incluyan nombres que comiencen por `viptela-reserved-`, como se muestra en este ejemplo:

```
29-Sep-2026 23:11:13,952 CDT [] [vManage-new] [UserUtils] (default task-127462) |default| Request Store
```



Nota: Las cuentas de servicio del sistema reservadas `viptela` se documentan en la sección Autenticación, Autorización y Contabilización de la Guía de Configuración de Interfaces y Sistemas SD-WAN de Cisco Catalyst.

Interpretar resultados y documentos para TAC

Si no se encuentra ninguna de estas entradas:

- No se detectaron indicadores de compromiso en este registro de este administrador
- Documente este resultado para su caso TAC
- Repita ambas comprobaciones en los jefes restantes

Si se encuentran estas entradas:

- Esto puede indicar posibles indicadores de compromiso
- Documentar todas las conclusiones y abrir un caso TAC inmediatamente
- Incluya las entradas de registro y las marcas de tiempo de su caso, junto con los resultados de la verificación 1 para el mismo período de tiempo
- TAC realiza la determinación de evaluación oficial

Preguntas Frecuentes

A: ¿Cuál es el primer paso para abordar este aviso de seguridad?

R: Recopile los archivos de administración y tecnología de todos los jefes (vManage) y, a continuación, actualice todos los jefes a una versión de software fija. Después de actualizar, abra un caso TAC y cargue los técnicos administrativos para que TAC pueda analizar su entorno en busca de indicadores de compromiso.

A: ¿Qué componentes se ven afectados por esta asesoría?

R: Solo se ve afectado Cisco Catalyst SD-WAN Manager (vManage).

A: ¿También necesitamos actualizar los controladores, validadores o routers de borde?

R: No, no para hacer frente a este aviso. Actualice todos los jefes (vManage) a una versión fija y utilice la [matriz de compatibilidad de controladores](#) para confirmar que la nueva versión de Manager es compatible con los demás componentes.

A: ¿Hay alguna solución alternativa disponible?

R: No. No hay soluciones alternativas para esta vulnerabilidad. Actualice a una versión fija.

A: ¿A qué versión necesito actualizar?

R: Actualice lo antes posible a la primera versión fija de su tren de versión actual. Consulte la tabla [Versiones fijas de software](#) en este documento. TAC confirma la versión adecuada para su entorno específico.

A: Ya he actualizado a una versión fija para un aviso de seguridad SD-WAN anterior. ¿Tengo que actualizar de nuevo?

R: Sí, a menos que su versión actual sea igual o posterior a la primera versión fija de su tren en la tabla [Versiones fijas de software](#). Las versiones fijas de los avisos anteriores no incluyen necesariamente la corrección de esta vulnerabilidad.

A: ¿Tengo que recopilar técnicos de administración de todos los gerentes?

R: Yes. TAC requiere archivos de tecnología de administración de todos los administradores (vManage), incluidos todos los miembros del clúster y todos los administradores de un sitio de recuperación ante desastres (DR), para evaluar correctamente su entorno.

A: ¿Puedo comprobar yo mismo los indicadores de compromiso?

R: Yes. Si no puede recopilar archivos de administración y tecnología, utilice los [Pasos de verificación manual](#) en cada administrador y comparta los resultados con el TAC. La recolección de tecnología administrativa sigue siendo el método preferido, y el TAC toma la determinación oficial de la evaluación.

A: ¿Cómo determina el TAC si mi sistema se ha visto comprometido?

R: El TAC analiza los archivos técnicos de administración mediante herramientas especializadas para evaluar su entorno en busca de indicadores de compromiso.

A: ¿Qué ocurre si se identifican indicadores de compromiso?

R: El TAC se pone en contacto con usted para hablar sobre los siguientes pasos y la orientación específica para su entorno. Cisco no lleva a cabo la remediación en su nombre. TAC proporciona la orientación necesaria para que pueda continuar.

A: ¿Puedo iniciar la actualización antes de que el TAC analice mis técnicos administrativos?

R: Yes. Recopile técnicos de administración, actualice a una versión fija y luego abra un caso TAC para que TAC pueda escanear los técnicos de administración en busca de indicadores de compromiso.

A: ¿Se espera tiempo de inactividad durante la remediación?

R: El impacto depende de la arquitectura de implementación y de la ruta de remediación. El TAC proporciona orientación sobre cómo minimizar el impacto del servicio durante el proceso.

A: Tengo una superposición de SD-WAN alojada en la nube. ¿Cuáles son mis opciones de actualización?

R: Para las superposiciones alojadas en la nube, los clientes tienen dos opciones:

1. Compruebe si su entorno está programado para una actualización automatizada. Para ello, vaya a SSP > Detalles de superposición > Cambiar ventanas.
2. Si no desea esperar a la actualización programada, tiene dos opciones:
 - Realice la actualización por sí mismo utilizando las guías de actualización disponibles en este documento.
 - Abra un caso de TAC en espera para su ventana de mantenimiento preferida. El TAC está disponible para ayudarle en caso de que tenga dificultades con la actualización.

A: Somos una superposición alojada por Cisco. ¿Tenemos que revisar las reglas de acceso en el SSP?

R: Se recomienda a todos los clientes alojados en Cisco que revisen sus propias reglas de entrada permitidas en SSP > Detalles de superposición > Permitir reglas de entrada y que se aseguren de que solo se permiten los prefijos necesarios de su lado. Estas reglas son solo para el acceso a la administración y no se aplican a los routers de borde.

A: ¿Proporciona Cisco TAC servicios de análisis de diagnóstico o de investigación para esta vulnerabilidad?

R: El Cisco TAC puede ayudar a los clientes buscando indicadores de compromiso (IoC) relacionados con esta vulnerabilidad. Sin embargo, el TAC no realiza análisis forenses exhaustivos ni investigaciones de incidentes. Para llevar a cabo un trabajo de diagnóstico completo o investigaciones de seguridad detalladas, recomendamos que los clientes contraten a su empresa de respuesta ante incidentes (IR) de terceros preferida.

A: ¿Cuáles son las prácticas recomendadas generales o las formas de reducir las vulnerabilidades de mi superposición de SD-WAN?

R: Consulte la [Guía de endurecimiento de SD-WAN de Cisco Catalyst](#) para conocer las mejores prácticas y recomendaciones para reducir las vulnerabilidades en su superposición de SD-WAN.

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).