Remediar el aviso de seguridad de Catalyst SD-WAN - Junio de 2026

Contenido

Introducción

Este documento describe los pasos para identificar y abordar las vulnerabilidades de seguridad críticas en SD-WAN basándose en los avisos PSIRT del 4 de junio de 2026.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Arquitectura Cisco Catalyst SD-WAN y componentes de control (vManage, vSmart, vBond)
- 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.

Estos consejos están disponibles en los siguientes enlaces:

- Vulnerabilidad de escalación de privilegios autenticados de Cisco Catalyst SD-WAN Manager

Estos defectos se abordan en las siguientes recomendaciones PSIRT:

- ID de bug de Cisco CSCwu18563

Flujo de trabajo de remediación

Este aviso describe una vulnerabilidad de escalado de privilegios en el Administrador de SD-WAN que requiere privilegios de netadmin para aprovecharse de ella.

Según el aviso, las rutas conocidas para que un atacante remoto no autenticado obtenga esos privilegios son la explotación de CVE-2026-20182 (cisco-sa-sdwan-rpa2-v69WY2SW) o CVE-2026-20127 (cisco-sa-sdwan-rpa-EHchtZk).

Si los componentes de control se han actualizado a una versión fija para ambos asesores y Cisco no identificó ningún indicador de compromiso (IoC) potencial en los archivos de administración y tecnología que proporcionó para los eventos anteriores, las rutas de explotación no autenticadas conocidas para esta nueva vulnerabilidad se mitigan en esos dispositivos específicos, según los archivos revisados.

Esto no elimina la exposición cuando un atacante tiene credenciales de netadmin válidas. Cisco aún no ha publicado una solución de software para esta vulnerabilidad y no hay soluciones alternativas disponibles; a medida que se disponga de ellas, se ofrecerán más orientaciones.

Acción requerida:abra un caso de Cisco TAC para abordar este aviso de seguridad.

TAC está disponible para:

- Evalúe su entorno en busca de indicadores de compromiso
- Le guiará por la ruta de solución adecuada en función de la evaluación.
- Proporcionar orientación sobre los siguientes pasos que se deben dar si se identifican indicadores de compromiso

1. Recopile Admin-Techs: ejecute admin-tech en todos los componentes de control (vSmart, vManage, vBond). vSmart admin-techs no se debe ejecutar simultáneamente: ejecútelos de uno en uno. Todos los demás pueden recogerse en cualquier orden. Seleccione las opciones Log (Registro) y Tech (Tecnología). El núcleo no es necesario.
2. Abra el caso del TAC: comuníquese con el TAC de Cisco y proporcione todos los paquetes de registro de tecnología de administración de componentes de control.
3. Evaluación del TAC: realiza una evaluación preliminar de los indicadores de compromiso dentro de su entorno y el TAC realiza una evaluación preliminar de los indicadores de compromiso en su entorno.
4. Ejecutar remediación: complete el proceso específico proporcionado por el TAC si es necesario.

Paso 1: Recopilar archivos técnicos de administración de todos los componentes de control

required (obligatorio): Recopile los archivos de administración y tecnología de todos los componentes de control antes de realizar cualquier actualización o cambio de configuración para conservar los datos de diagnóstico y cualquier posible indicador de compromiso (IoC). El TAC utiliza estos archivos en el paso 3 para analizar su entorno.

Colección: Para la generación de tecnología de administración, seleccione Log and Tech options (Opciones de registro y tecnología). El núcleo no es necesario.

1. Ejecute admin-tech en ALL Controllers (vsmarts): no ejecute estos controladores simultáneamente; recolectar uno a la vez
2. Ejecute admin-tech en ALL Managers (vManagers)
3. Ejecute admin-tech en ALL Validators (vBonds)

Recopile una Admin-Tech en un entorno SD-WAN y cárguela en un caso TAC

Nota: TAC analiza estos archivos para evaluar su entorno en busca de indicadores de compromiso relacionados con este aviso. El análisis de este aviso se centra en una entrada de registro específica que no distingue entre uso legítimo y uso malintencionado; se requiere una revisión manual por parte del TAC.

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

Para los clientes que no pueden compartir archivos de administración y tecnología, hay disponible

un paso de verificación manual. Este paso proporciona un indicador preliminar que debe documentarse y compartirse con el TAC.

Consulte la sección Pasos de Verificación Manual al final de este documento para ver el procedimiento detallado. Documente todas las conclusiones y proporciónelas al TAC en su caso de soporte.

Paso 2: Abra un caso TAC y cargue archivos técnicos de administración

Después de recopilar técnicos de administración en el paso 1, abra un caso de soporte del TAC de Cisco y cargue los archivos técnicos de administración recopilados. El TAC analiza los técnicos administrativos en busca de indicadores de compromiso asociados a este aviso.

Acciones necesarias:

1. Abra un caso TAC de Gravedad 3 con "CVE-2026-20245" y el ID de asesoramiento `cisco-sa-sdwan-privesc-4uxFrdzx` en el título para iniciar el análisis.
2. Cargue TODOS los paquetes de registro de tecnología de administración recopilados en el paso 1 (Controladores, administradores y validadores).
3. Espere a que el TAC complete el análisis y comunique los resultados.

Nota: Cisco no ha publicado una solución de software para esta vulnerabilidad y no hay soluciones alternativas disponibles. El análisis del TAC del paso 3 ayuda a determinar si hay algún indicador de compromiso en los archivos de administración y tecnología que ha proporcionado. Seguirá una orientación más detallada a medida que se disponga de ella a través del departamento de ingeniería.

Paso 3: Evaluación del TAC

TAC realiza un análisis preliminar de los archivos admin-tech que cargó en el paso 2 y los evalúa para detectar indicadores de compromiso asociados con este aviso.

Para este aviso, el análisis se centra en una entrada de registro específica en `/var/log/scripts.log` en cada administrador (vManage). Debido a que el comando subyacente es legítimo y el registro no distingue entre uso legítimo y malintencionado, cualquier entrada coincidente requiere una revisión manual por parte del TAC en comparación con la posición operativa normal del cliente antes de ser tratada como un indicador confirmado.

Posibles resultados del análisis del TAC:

- No se identificaron entradas de registro coincidentes: según los archivos admin-tech revisados, no se observaron indicadores asociados con este aviso. Por el momento, no es

necesario adoptar ninguna otra medida específica en relación con esta recomendación. El resultado se limita a los archivos técnicos de administración recibidos y puede estar limitado por el período de retención de registros en cada dispositivo.
- Se han identificado entradas de registro coincidentes: TAC pondrá en contacto al cliente con pasos de revisión adicionales. Como Cisco no ha publicado una corrección de software para este aviso, la actualización por sí sola no resuelve esta vulnerabilidad. La guía del TAC para escenarios de compromiso confirmado se documenta en los artículos TechZone relacionados a los que se hace referencia en el Paso 4.

Nota: Según el aviso, la explotación de esta vulnerabilidad requiere privilegios de netadmin, que un atacante no autenticado puede obtener solo mediante credenciales válidas o la explotación de CVE-2026-20182 o CVE-2026-20127. Si los componentes de control se han actualizado a una versión fija para ambos avisos y no se identificaron indicadores de compromiso para los eventos anteriores, las rutas de explotación no autenticadas conocidas para esta nueva vulnerabilidad se mitigan en esos dispositivos específicos, según los archivos revisados.

Paso 4: Si se identifican indicadores de compromiso, siga las directrices del TAC

Si el TAC identifica indicadores de compromiso asociados a este aviso en su entorno, el TAC se pone en contacto con usted para ofrecerle orientación específica. Complete todas las instrucciones proporcionadas por el TAC.

Si no se identifican indicadores de compromiso para esta asesoría, no se requiere ninguna otra acción específica para esta asesoría en este momento, según los archivos técnicos de administración revisados.

Importante: Cisco no ha publicado una corrección de software para este aviso y no hay soluciones alternativas disponibles. Debido a que la explotación de esta vulnerabilidad requiere privilegios de netadmin obtenidos a través de CVE-2026-20182 o CVE-2026-20127, los clientes deben asegurarse de que la remediación de esos avisos anteriores esté completa. Consulte los documentos correspondientes para obtener información sobre el flujo de remediación establecido:

Consideraciones

Una vez concluida la remediación con éxito, y en función de los requisitos de garantía de seguridad específicos de cada cliente, es posible que los clientes deseen evaluar las siguientes

actividades de higiene y actuar en consecuencia. Estas actividades se aplican independientemente de la opción de remediación seleccionada. Están gestionadas por el cliente; Cisco no los dirige ni los lleva a cabo en nombre del cliente.

- Revisión de todas las cuentas de usuario locales
- Rotación de credenciales
- Rotación de los secretos presentes en las configuraciones de los dispositivos, por ejemplo (lista no exhaustiva):
  - Credenciales para cuentas de usuario locales
  - Identificaciones de comunidad SNMP
  - claves secretas TACACS
  - Certificados y claves previamente compartidas de VPN
  - Claves SSH de confianza
- Revisión de plantillas de configuración

Dispositivos periféricos: Sospecha de riesgo

Cisco no recomienda una ruta de remediación concreta; la selección de una opción de solución corresponde al cliente. Como nota informativa para los clientes que evalúan su entorno: cuando el cliente sospeche que un dispositivo periférico está en peligro, un restablecimiento de fábrica y la reincorporación de los dispositivos periféricos afectados es una acción gestionada por el cliente que este podría tener en cuenta al realizar su selección. La decisión sobre si seguir este enfoque y qué opción seleccionar corresponde al cliente.

El comando adecuado para realizar un restablecimiento de fábrica seguro es:

```
factory-reset all secure 3-pass
```

Versiones de software fijas

⚠ Importante: En el momento de la publicación de este documento, Cisco no ha publicado una corrección de software que se refiera a CVE-2026-20245. Según el aviso, Cisco planea abordar esta vulnerabilidad en Cisco Catalyst SD-WAN Manager en una futura versión. No hay soluciones alternativas. Esta sección se actualizará cuando el software fijo esté disponible.

Debido a que el aprovechamiento de esta vulnerabilidad requiere privilegios de netadmin que un atacante no autenticado solo puede obtener a través de CVE-2026-20182 o CVE-2026-20127, se recomienda a los clientes que se aseguren de que sus componentes de control estén ejecutando una versión fija para esos avisos anteriores. Las versiones fijas de estas recomendaciones se documentan en el aviso de seguridad de SD-WAN del 14 de mayo de 2026 y en el documento

TechZone correspondiente:

- Vulnerabilidad de omisión de autenticación del controlador Cisco Catalyst SD-WAN (14 de mayo de 2026)
- (Tabla Versiones de software fijas)

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: El método preferido es la colección Admin-tech. Utilice solamente el paso de verificación manual a continuación si los archivos admin-tech no se pueden recolectar y compartir con el TAC. El resultado de este paso manual es preliminar; documentar las conclusiones y compartirlas con el TAC, que realiza la evaluación oficial.

Nota: Para este aviso, la verificación manual consiste en una única comprobación de registro dirigida. La entrada de registro buscada es generada por un comando legítimo y el registro por sí solo no distingue entre uso legítimo y malicioso. Cualquier dato coincidente debe revisarse en relación con la posición operativa normal del cliente antes de considerarlo un posible indicador. Si una entrada coincidente no se puede conciliar con las operaciones normales, documente la conclusión y compártala con el TAC.

Verificación: Verifique `scripts.log` en cada Administrador (vManage) para las Entradas de Carga de Lista de Arrendatarios

Según el aviso de PSIRT, se recomienda a los clientes que auditen el archivo `scripts.log`, ubicado en `/var/log/`, para entradas similares al siguiente ejemplo:

```
Apr 15 09:44:57 vmanage vScript: Tenant list upload per vsmart serial number: /usr/bin/vconfd_script_up
```

Paso 1: Acceda a vshell en cada administrador (vManage) y busque el archivo de registro

En la CLI de vManage, vaya a vshell y ejecute:

```
vs
zgrep "vconfd_script_upload_tenant_list.sh" /var/log/scripts.log*
```

Repita la comprobación en cada vManage de la implementación (incluidos todos los miembros del clúster y cualquier vManage emparejado con DR).

Paso 2: Interpretar resultados y documentos para TAC

Si NO se devuelven entradas coincidentes:

- No se observaron indicadores de compromiso asociados con este aviso en el archivo de registro de este dispositivo.
- Documente este resultado para su caso TAC (incluya el nombre de host del dispositivo y la fecha/rango de los archivos de registro buscados).
- Continúe con la comprobación de los jefes restantes.

Si se devuelven entradas coincidentes:

- Cada entrada coincidente debe revisarse teniendo en cuenta la posición operativa normal del cliente. El comando subyacente (carga de lista de arrendatarios) es legítimo y puede aparecer durante las operaciones rutinarias.
- Para cada entrada coincidente, capture la marca de tiempo, la línea de registro completa y la ruta de archivo a la que se hace referencia después de la `ruta -cli`.
- Si una entrada coincidente no se puede conciliar con una operación conocida y legítima, puede ser un indicador de riesgo. Documente el resultado y proporciónelo al TAC para su revisión.
- Documentar todas las conclusiones y abrir un caso TAC. Incluya las entradas de registro coincidentes y el resultado del comando source en su caso.
- El TAC realizará la evaluación oficial. Si la evaluación identifica indicadores de compromiso, siga el flujo descrito en los documentos relacionados de TechZone: y las guías de remediación.

Preguntas Frecuentes

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

R: Recopile archivos de tecnología de administración de todos los componentes de control (vSmart, vManage, vBond) antes de realizar cualquier actualización o cambio de configuración para conservar los datos de diagnóstico y cualquier posible indicador de compromiso. A continuación, abra un caso del Cisco TAC y cargue los técnicos administrativos para que el TAC pueda analizarlos.

A: ¿Ha publicado Cisco una solución de software para esta vulnerabilidad?

R: No en el momento de la publicación de este documento. Según el aviso, Cisco tiene previsto abordar esta vulnerabilidad en Cisco Catalyst SD-WAN Manager en una futura versión. No hay

soluciones alternativas. Este documento se actualizará cuando esté disponible una versión fija.

A: Si no hay solución, ¿por qué recomienda Cisco realizar alguna acción ahora?

R: La explotación de esta vulnerabilidad requiere privilegios de netadmin. Según el aviso, un atacante no autenticado puede obtener esos privilegios sólo a través de credenciales válidas o mediante la explotación de CVE-2026-20182 o CVE-2026-20127. Garantizar que los componentes de control se actualizan a las versiones fijas de esos avisos anteriores dirige las rutas no autenticadas conocidas para obtener los privilegios necesarios para explotar esta vulnerabilidad. El análisis técnico-administrativo del paso 3 ayuda a determinar si hay algún indicador de compromiso en los archivos revisados.

A: ¿Necesito recopilar técnicos de administración de todos los componentes de control?

R: Yes. TAC requiere archivos de tecnología de administración de todos los controladores (vSmart, recopilados de uno en uno), todos los administradores (vManage) y todos los validadores (vBond) para realizar el análisis.

A: ¿Cómo determina el TAC si mi sistema tiene indicadores de compromiso asociados a este aviso?

R: TAC revisa los archivos admin-tech y busca la entrada de registro específica descrita en el aviso de PSIRT en `/var/log/scripts.log` en cada administrador. El comando subyacente es legítimo; todas las entradas que coincidan deben revisarse en función de su estado de funcionamiento normal antes de ser tratadas como un indicador potencial. El TAC realiza esa revisión.

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

R: El TAC se pone en contacto con usted para ofrecerle orientación específica. Dado que actualmente no hay ninguna corrección de software disponible para este aviso, la actualización por sí sola no resuelve un riesgo confirmado. La guía del TAC sigue el flujo documentado en los artículos relacionados de TechZone para las recomendaciones de mayo de 2026 y febrero de 2026.

A: ¿Los routers periféricos (Cisco IOS XE) se ven afectados por este aviso?

R: Este aviso afecta a Cisco Catalyst SD-WAN Manager. Según el aviso, Cisco ha observado casos limitados en los que el aprovechamiento de esta vulnerabilidad ha dado lugar a un cambio de configuración empujado a los dispositivos periféricos; se recomienda a los clientes que verifiquen la configuración de sus dispositivos periféricos.

A: ¿Qué tipos de implementación se ven afectados?

R: Según el aviso, esta vulnerabilidad afecta a todos los tipos de implementación de Cisco Catalyst SD-WAN Manager independientemente de la configuración del dispositivo, incluida la implementación in situ, Cisco SD-WAN Cloud-Pro, Cisco SD-WAN Cloud (gestionada por Cisco) y Cisco SD-WAN para instituciones gubernamentales (FedRAMP).

A: Ya he actualizado las recomendaciones de mayo de 2026 y febrero de 2026 y no se han identificado indicadores de compromiso para estos eventos. ¿Estoy expuesto a esta nueva vulnerabilidad?

R: Si sus componentes de control están ejecutando una versión fija para CVE-2026-20182 y CVE-2026-20127 y no se identificaron indicadores de compromiso para esos eventos anteriores en los archivos admin-tech revisados, las rutas de explotación no autenticadas conocidas para esta nueva vulnerabilidad se mitigan en esos dispositivos específicos, según los archivos revisados. Esto no elimina la exposición cuando un atacante posee credenciales válidas de netadmin.

A: ¿Puedo realizar la verificación yo mismo en lugar de esperar al TAC?

R: Los clientes que no pueden compartir técnicos administrativos pueden realizar el paso de verificación manual descrito en el Apéndice. El resultado es preliminar; documentar las conclusiones y compartirlas con el TAC, que realiza la evaluación oficial.

A: ¿Cuáles son las prácticas recomendadas generales para reforzar mi superposición SD-WAN?

R: Consulte la Guía de Consolidación de Cisco Catalyst SD-WAN para conocer las prácticas recomendadas.

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

R: Cisco TAC puede ayudar a los clientes revisando los archivos técnicos de administración para encontrar los indicadores de compromiso documentados en el aviso de PSIRT. Cisco TAC no realiza análisis de diagnóstico en profundidad ni investigaciones de incidentes. Para llevar a cabo un trabajo de diagnóstico completo o investigaciones de seguridad detalladas, se recomienda a los clientes que contraten a su empresa de respuesta ante incidentes (IR) de terceros preferida.

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).