

# Remediar el aviso de seguridad de Catalyst SD-WAN: febrero de 2026

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Flujo de trabajo de remediación](#)

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

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

[Paso 2: Abra un caso TAC y cargue archivos técnicos de administración](#)

[Paso 3: Evaluación del TAC](#)

[Paso 4: Ejecución de la remediación \(guiada por TAC\)](#)

[Ruta A: No se han encontrado indicadores de compromiso: actualización](#)

[Ruta B: Indicadores de compromiso identificados \(guiados por PSIRT\)](#)

[Versiones de software fijas](#)

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

[Verificación 1: Verifique si hay Logins SSH No Autorizados en los Logs de Autenticación](#)

[Verificación 2: Comprobar conexiones de pares no autorizadas en registros del sistema del controlador](#)

[Preguntas Frecuentes](#)

---

## Introducción

Este documento describe los pasos para identificar y solucionar vulnerabilidades de seguridad críticas en SD-WAN basándose en los avisos PSIRT del 25 de febrero 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:

- [Vulnerabilidades de la SD-WAN de Cisco Catalyst](#)
- [Vulnerabilidad de omisión de autenticación del controlador Cisco Catalyst SD-WAN](#)

Estos defectos se abordan en las siguientes recomendaciones PSIRT:

- ID de bug de Cisco [CSCws52722](#)
  - ID de bug de Cisco [CSCws33583](#)
  - ID de bug de Cisco [CSCws33584](#)
  - ID de bug de Cisco [CSCws33585](#)
  - ID de bug de Cisco [CSCws33586](#)
  - ID de bug de Cisco [CSCws33587](#)
  - ID de bug de Cisco [CSCws93470](#)
- 

## Flujo de trabajo de remediación



Nota: Todas las implementaciones de SD-WAN son vulnerables y requieren una acción inmediata. Sin embargo, no todos los sistemas muestran evidencia de compromiso.

---

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.
- Trabajar con el equipo PSIRT si se identifican indicadores de compromiso
- Proporcionar asistencia y orientación para la actualización si no se detectan indicadores de compromiso.

1. Collect 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. Abrir caso de TAC: comuníquese con Cisco TAC y proporcione todos los paquetes de registro de tecnología de administración de componentes de control
  3. Evaluación del TAC: el TAC evalúa su entorno en busca de indicadores de compromiso
  4. Ejecutar remediación: complete el proceso específico proporcionado por el TAC
- 

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

required (obligatorio): Recopile archivos técnicos de administración de todos los componentes de control antes de abrir su caso TAC. Esto es esencial para que el TAC evalúe su entorno.

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



Nota: Los vSmart admin-techs no se deben ejecutar simultáneamente: recójelos de uno en uno. Los técnicos de administración para gerentes y validadores se pueden recopilar en cualquier orden.

---

[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 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: Abra un caso TAC y cargue archivos técnicos de administración

Después de recopilar todos los archivos técnicos de administración del paso 1, abra un caso de soporte del TAC de Cisco.

Acciones necesarias:

1. Abra un caso TAC con el nivel de gravedad adecuado para el impacto de su negocio
  2. Cargue TODOS los paquetes de registro de tecnología de administración recopilados en el paso 1 (Controladores, administradores y validadores)
  3. Hacer referencia a los avisos PSIRT
  4. Espere a la evaluación y orientación del TAC
- 



Precaución: El TAC determina el estado de su sistema y recomienda los siguientes pasos adecuados.

No intente realizar más pasos sin la guía del TAC

---

## Paso 3: Evaluación del TAC

El TAC analiza los archivos técnicos de administración cargados y determina el estado de su sistema.

Durante este tiempo:

- Antes de emprender cualquier acción, espere a recibir una evaluación oficial del TAC
  - El TAC se pone en contacto con usted para comunicarle sus conclusiones y los siguientes pasos
- 

## Paso 4: Ejecución de la remediación (guiada por TAC)

El TAC le guía a través del proceso de remediación adecuado en función de su evaluación. Complete todas las instrucciones proporcionadas por el TAC.

## Ruta A: No se han encontrado indicadores de compromiso: actualización

Si el TAC confirma que no hay evidencia de compromiso, actualice a la versión de software fija. Seleccione la versión adecuada de la tabla [Versiones fijas de software](#) de este documento y haga referencia a la guía de actualización vinculada en esta sección.



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](#)

## Ruta B: Indicadores de compromiso identificados (guiados por PSIRT)

Si el TAC confirma que existen indicadores de compromiso, se pone en contacto con el equipo PSIRT para desarrollar una estrategia de remediación personalizada y específica para su entorno. Complete todas las directrices proporcionadas por el TAC y PSIRT.

## Versiones de software fijas

Estas versiones de software contienen correcciones para las vulnerabilidades identificadas:

Se aplica a las versiones actuales	Versión fija	Software disponible
20.3, 20.6, 20.9	20.9.8.2 *	<a href="#">20.9.8.2 imágenes de actualización para vManage, vSmart y vBond</a>
20.10, 20.11, 20.12.5 y anteriores en 20.12	20.12.5.3	<a href="#">20.12.5.3 imágenes de actualización para vManage, vSmart y vBond</a>
20.12.6	20.12.6.1	<a href="#">20.12.6.1 imágenes de actualización para vManage, vSmart y vBond</a>
20.13, 20.14 y 20.15.x	20.15.4.2	<a href="#">20.15.4.2 imágenes de actualización para vManage, vSmart y vBond</a>
20.16, 20.17 y 20.18.x	20.18.2.1	<a href="#">20.18.2.1 imágenes de actualización para vManage, vSmart y vBond</a>



Nota: Para los clientes de CDCS (clúster alojado en Cisco), 20.15.405 es también una

---

versión fija. Esto se aplica específicamente a la implementación de clústeres alojados por Cisco y se gestiona por separado de la ruta de actualización estándar.

---

\* Si se encuentra en la versión 20.9 o anterior: El software fijo para su versión (20.9.8.2) está disponible el 27/02. Cisco recomienda permanecer dentro de su versión principal actual y esperar a la versión 20.9.8.2 en lugar de actualizar a una versión principal superior (20.12, 20.15, 20.18). Si actualmente se encuentra en una versión inferior a 20.9, espere a que 20.9.8.2 se actualice allí. Continúe trabajando con el TAC y vuelva a consultar el enlace de software disponible el 27 de febrero.

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 componentes del control.

### Verificación 1: Verifique si hay Logins SSH No Autorizados en los Logs de Autenticación

Paso 1: Identificar direcciones IP del sistema vManage válidas

Acceda a cada controlador vSmart y ejecute:

```
west-vsmart# show control connections | inc "vmanage|PEER|IP"
```

Ejemplo de salida:

INDEX	PEER TYPE	PEER PROT	PEER SYSTEM IP	SITE ID	DOMAIN ID	PEER PRIV PRIVATE	PEER IP	PORT	PUB PUBLIC I
0	vmanage	dtls	10.1.0.18	101018	0	10.1.10.18		12346	10.1.10.1

Paso 2: Generar cadena de expresión regular (sólo vBond y vSmart)

Combine todas las IP del sistema del paso 1 en un patrón de regex OR:

```
system-ip1|system-ip2|...|system-ipn
```

Paso 2b: Paso adicional para sistemas vManage

Si ejecuta estos comandos en el propio vManage, añada la IP de host local (127.0.0.1), la IP del sistema local, todas las IP de clúster y la IP de la interfaz de transporte VPN 0 al regex:

```
system-ip1|system-ip2|...|system-ipn|127.0.0.1|
```

Para buscar la dirección IP del sistema vManage local, utilice:

```
show control local-properties
```

Para buscar la IP de la interfaz de transporte VPN 0 y la IP del clúster, utilice:

```
show interface | tab
```

### Paso 3: Ejecutar comando de verificación

Ejecute este comando, reemplazando REGEX con su cadena regex del Paso 2:

```
west-vsmart# vs
west-vsmart:~$ zgrep "Accepted publickey for vmanage-admin from " /var/log/auth.log* | grep -vE "\s(REG
```



Nota: Este comando filtra los registros de autenticación para mostrar solamente los inicios de sesión de vmanage-admin de orígenes inesperados. Los inicios de sesión legítimos solo deben originarse en direcciones IP relacionadas con vManage.

---

### Paso 4: Interpretar resultados y documentos para TAC

Si se muestra NO output:

- No se detectaron indicadores de compromiso en este dispositivo
- Documente este resultado para su caso TAC
- Continuar la evaluación de los controladores restantes

Si se imprimen líneas de registro:

- Examine cuidadosamente cada dirección IP mostrada
- Verifique que la IP no esté relacionada con la infraestructura de vManage (IP del clúster, IP del sistema antiguo o similar)
- Si no puede identificar la IP de origen como legítima, esto puede indicar posibles indicadores de compromiso
- La entrada del registro muestra una marca de tiempo y una dirección IP de origen
- Documentar todas las conclusiones y abrir un caso TAC inmediatamente
- Incluya las entradas de registro, las marcas de tiempo y las IP de origen en su caso
- TAC realiza la determinación de evaluación oficial

### Verificación 2: Comprobar conexiones de pares no autorizadas en registros del sistema del controlador

Este comando extrae todos los pares peer-type e peer-system-ip de los archivos syslog del controlador y los genera como una lista para que la revise. No marca automáticamente entradas sospechosas: debe inspeccionar la salida y determinar si cada IP del sistema de peer es una parte conocida y legítima de su infraestructura SD-WAN. Ejecute esto en todos los componentes del control (controladores, administradores y validadores).

Paso 1: Ejecute el comando en cada componente del control:

Primero, acceda a vshell y navegue hasta el directorio de registro:

```
vs
cd /var/log
```

A continuación, ejecute el comando this:

```
awk '{
  match($0, /peer-type:([a-zA-Z0-9]+)[^ ]* peer-system-ip:([0-9.:]+)/, arr);
  if(arr[1] && arr[2]) print "(" arr[1] ", " arr[2] ")";
}' vsyslog* | sort | uniq
```

## Paso 2: Interpretar resultados y documentos para TAC

Si el resultado solo muestra direcciones IP del sistema vManage/vSmart/vBond conocidas:

- No se detectaron indicadores de compromiso en esta comprobación
- Documente este resultado para su caso TAC
- Continuar la evaluación de los componentes de control restantes

Si el resultado contiene IPs del sistema de peer no reconocidas:

- Examine cuidadosamente cada dirección IP y el tipo de par que se muestra
- Verifique que la IP no esté relacionada con su infraestructura de plano de control SD-WAN conocida
- 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 el resultado completo del comando con pares peer-type y peer-system-ip en su caso
- TAC realiza la determinación de evaluación oficial

---

## Preguntas Frecuentes

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

R: Recopile archivos de administración y tecnología de todos los componentes de control y abra un caso TAC para cargar los archivos. El TAC evalúa su entorno y proporciona orientación sobre los siguientes pasos.

P. ¿A qué versión debo actualizar?

R. Actualice a la versión fija más cercana lo antes posible.

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

R: Sí, 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 evaluar correctamente su entorno.

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 el equipo PSIRT y 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: ¿Cómo sé qué versión de software fija debo utilizar?

R: Consulte la tabla [Versiones fijas de software](#) en este documento. TAC confirma la versión adecuada para su entorno específico.

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

R: No, espere a que el TAC complete su evaluación y proporcione orientación antes de intentar cualquier acción de remediación.

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: ¿Se incluyen las correcciones de PSIRT en la próxima versión 20.15.5 y en otras próximas versiones?

R: Sí, las correcciones se incluyen en 20.15.5 y en otras versiones futuras. Sin embargo, la actualización para mitigar las vulnerabilidades descritas en este documento debe priorizarse **INMEDIATAMENTE**. (¡No espere!)

A: ¿Es necesario actualizar todos los controladores en caso de que no se encuentren indicadores de compromiso?

R: Sí, todos los componentes de control de SD-WAN (vManage, vSmart y vBond) deben actualizarse a una versión de software fija. No es suficiente actualizar sólo un subconjunto de controladores.

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 le ayudará si tiene dificultades con la actualización.

A: ¿También necesitamos actualizar los routers de extremo?

R: Este aviso no afecta a los dispositivos Cisco IOS XE.

P.: Somos una solución de superposición alojada de Cisco. ¿Tenemos que corregir alguna ACL o realizar alguna acción en el SSP?

R: Se recomienda a todos los clientes alojados en Cisco que revisen sus propias reglas de entrada permitidas en SSP y que se aseguren de que sólo se permiten los prefijos necesarios de su parte. Estas reglas son solo para el acceso a la administración y no se aplican a los routers de borde. Revíselas en SSP > Detalles de superposición > Permitir reglas de entrada. Tenga en cuenta que el puerto 22, 830 siempre estaba bloqueado de forma predeterminada el día 0 de aprovisionamiento por parte de Cisco desde el exterior a los controladores alojados en la nube.

P: Trabajamos en CDCS/arrendatario compartido. ¿A qué versión se va a actualizar?

R: En función de la versión actual, los clústeres de Shared Tenant o CDCS se actualizarán según lo programado o bien ya se actualizarán a las versiones fijas. A continuación se indican el arrendatario compartido y las versiones fijas de CDCS:

1. Clústeres de Early Adopter => 20.18.2.1 (en realidad es lo mismo que la versión estándar)

2. Clústeres de versión recomendados => 20.15.405 (versión específica de CDCS con correcciones de PSIRT)

Los clientes de CDCS no necesitan realizar ninguna acción eficaz para abordar este PSIRT.

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.

A: Vemos los registros de un usuario "root" en nuestro sistema. ¿Deberíamos preocuparnos por esto?

R: Compruebe qué más está sucediendo en el sistema en ese momento. Estos registros son totalmente esperables. Por ejemplo, los registros de cambio de inicio de sesión del sistema de un usuario "root" se ven cuando se generan admin-techs. Los registros también se pueden ver desde un usuario "root" durante un reinicio.

user-name:"root" user-id:245 generated-at:2-28-2026T23:3:44

Feb 28 23:03:47 Manager01 SYSMGR[863]: %Viptela-Manager01-sysmgrd-6-INFO-1400002: Notification: system-

user-name:"root" user-id:248 generated-at:2-28-2026T23:3:47

---

## 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).