

Comprobar si hay negrita para los artículos ya existentes

Contenido

[Introducción](#)

[Referencias — Documentación de Cisco SD-WAN CVE-2026-20182](#)

[Correos electrónicos](#)

[Sherlock 1 - Entrada - Solicitar actualización & Admin-Tech Files](#)

[Sherlock 2 - Resultado - No se observaron IoC \(por archivo\)](#)

[Sherlock 3 - Recordatorio - Faltan archivos de Admin-Tech](#)

[TAC 1 - Investigación - Se requiere una revisión adicional \(se sospecha de IoC\)](#)

[TAC 2 - Resultado - No se han encontrado IoC \(confirmado por el ingeniero\)](#)

[TAC 3 - Validación - Confirmar propiedad de IP en superposición](#)

[TAC 4 - Resultado - Falsos positivos borrados](#)

[TAC 5 - Crítico - IoC identificado. llamada de revisión de programación](#)

[TAC 6 - Resultado - IoC duplicado \(Cerrar y redirigir\)](#)

[TAC 7 - Remediación - Seguimiento de opciones \(después de la llamada\)](#)

[TAC 8 - Remediación - Opciones actualizadas para estructuras en riesgo \(Opción 2 Seguimiento\)](#)

[TAC 17: hallazgo inverso. Anteriormente sin IoC, ahora IoC identificado \(CVE-2026-20182\)](#)

[CloudOps 1 - Proactivo - IoC detectado en Cloud Scan, se requiere tecnología administrativa para validar](#)

[Mensajes de correo electrónico para WAVE 2A para clientes que SUFRIERON UN IMPACTO ANTERIOR y que aún no han completado las opciones A, B o C. \(Las opciones 1 y 2 deben rehacerse\)](#)

[Plantilla de TAC 9 para sin COI para PSIRT2a/se reconstruyeron \(IMPACTADO PREVIAMENTE\)](#)

[Plantilla de TAC 10 para sí IOC para PSIRT2a/se reconstruyeron \(IMPACTADO PREVIAMENTE\)](#)

[Plantilla de TAC 11 para sin IOC para PSIRT2a/no se reconstruyeron \(IMPACTADO PREVIAMENTE\)](#)

[Plantilla de TAC 12 para sí IOC para PSIRT2a/no se reconstruyeron \(IMPACTADO PREVIAMENTE\)](#)

[Correos electrónicos para WAVE 2A para nuevos clientes \(no afectados anteriormente\)](#)

[Plantilla TAC 13 para no IOC/versión fija no disponible \(WAVE 2a — Await Fix\)](#)

[Plantilla de TAC 14 para versiones fijas o sin IOC disponibles \(WAVE 2a — Actualice ahora\)](#)

[Plantilla de TAC 15 para versiones de IOC identificadas/fijas disponibles \(WAVE 2a — Actualización urgente\)](#)

[Plantilla de TAC 16 para IOC identificado/versión fija no disponible \(WAVE 2a — Harden & Await Fix\)](#)

Introducción

Este documento centraliza las plantillas de correo electrónico aprobadas por el cliente que se utilizan durante la clasificación y la remediación de casos relacionados con la vulnerabilidad de omisión de autenticación del controlador Cisco Catalyst SD-WAN. Las plantillas se dividen por remitente: Sherlock (intercambio automatizado de casos que recopila datos técnicos de administración y devuelve los resultados preliminares de IoC) e ingeniero del TAC (seguimiento basado en el ser humano para la investigación, validación y orientación sobre soluciones).

Referencias — Documentación de Cisco SD-WAN CVE-2026-20182

Lista maestra de todos los documentos de Cisco a los que se hace referencia en las plantillas de correo electrónico anteriores. La numeración es unificada: superíndices por correo electrónico (p. ej. ^[2]) señale los elementos de esta lista.

1. **Guía de refuerzo de la SD-WAN de Cisco:** <https://sec.cloudapps.cisco.com/security/center/resources/Cisco-Catalyst-SD-WAN-HardeningGuide>
2. **Aviso oficial de seguridad (cisco-sa-sdwan-mltnps2-JxpWm7R) —**
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-mltnps2-JxpWm7R>
3. **Guía de remediación de TAC:** <https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/225842-remediate-catalyst-sd-wan-security.html#toc-h1d--1516256622>
4. **Guía de actualización de SD-WAN de Cisco:** <https://www.cisco.com/c/en/us/support/docs/wan/dpt/220424-upgrade-sd-wan-controllers-with-the-use.html>
5. **Guía de recopilación de tecnología de administración de Cisco SD-WAN —**
<https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/216954-how-to-collect-an-admin-tech-in-an-sd-wa.html>
6. **Segundo aviso de seguridad (cisco-sa-sdwan-rpa2-v69WY2SW) —**
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW>
7. **Inicie su actualización de Catalyst SD-WAN —** <https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/225515-start-your-catalyst-sd-wan-upgrade.html>

Correos electrónicos

Sherlock 1 - Entrada - Solicitar actualización & Admin-Tech Files

caso de uso

Alcance inicial cuando se abre un caso TAC para CVE-2026-20182 para aconsejar la recopilación de datos técnicos de administración de y luego actualizar todos los componentes de control SD-WAN.

Mensaje

Estimado cliente:

Gracias por ponerse en contacto con el Cisco Technical Assistance Center (TAC).

En cuanto a la vulnerabilidad asociada a **CVE-2026-20182**, consulte el [aviso oficial de seguridad](#)^[1] para obtener más información, así como la [Guía de remediación del TAC](#)^[2].

Nuestro objetivo principal es ayudar a proteger su entorno. Priorice **su planificación y ejecución de actualizaciones** como el paso más importante para mitigar este riesgo. Si aún no ha programado esta actualización, hágalo inmediatamente.

Recursos de actualización: Consulte el siguiente documento oficial de Cisco para obtener instrucciones detalladas sobre cómo realizar la actualización: [Guía de actualización para SD-WAN de Cisco](#)^[3]

Para habilitar la evaluación inicial de su entorno para cualquier posible indicador de compromiso (IoC) relacionado con CVE-2026-20182, debe realizar una recopilación de tecnología administrativa *antes* de realizar la actualización. Siga este orden de operaciones:

- 1. Recopilar archivos de Admin-Tech:** Genere los registros técnicos de administración de todos los componentes de control de SD-WAN antes de la actualización para asegurarse de que no se pierdan datos de diagnóstico. Asegúrese de seleccionar **"Registros"** y **"Tecnología"** al generar estos archivos.
 - **vsmarts (controladores):** Recopile uno a la vez, no simultáneamente.
 - **vBonds (validadores):** Recopilar de todos los nodos.
 - **Administrador (vManage):** Recopile datos de todos los nodos del clúster (DR activo y en espera).
- 2. Ejecutar actualización:** Actualice todos los componentes de control de SD-WAN (vManage, vSmart, vBond) a una versión de software fija enumerada en el aviso. No espere al análisis del registro de admin-tech antes de comenzar la actualización, ya que la actualización cierra la vulnerabilidad inmediatamente.
- 3. Cargar en caso TAC:** Una vez que se haya completado la actualización, cargue los archivos recopilados anteriormente en su caso TAC existente simultáneamente, si es posible. A continuación, nuestro equipo realizará un análisis de estos registros para evaluar su entorno en busca de indicadores de compromiso (IoC).

Recursos y asistencia:

Para obtener más información e instrucciones paso a paso sobre cómo generar y enviar de forma segura sus archivos admin-tech, consulte esta guía: [Guía de recopilación de tecnología de administración de Cisco SD-WAN](#)^[4].

Si tiene una suscripción a BCS/LCS, póngase en contacto con su Cisco NCE o Delivery Manager para obtener orientación adicional sobre el proceso de actualización o los siguientes pasos.

La privacidad y seguridad de sus datos siguen siendo nuestra máxima prioridad. Toda la información proporcionada se tratará de acuerdo con las políticas de privacidad y seguridad de Cisco.

Recibirá una confirmación automática por correo electrónico de **CADA** archivo cargado correctamente en el caso. asegúrese de revisar estas notificaciones.

Gracias por su rápida cooperación a la hora de proteger su infraestructura.

Enlaces:

- [1] [Aviso oficial de seguridad](#)
- [2] [Guía de remediación del TAC](#)
- [3] [Guía de actualización de SD-WAN de Cisco](#)
- [4] [Guía de recopilación de tecnología de administración de Cisco SD-WAN](#)

Saludos cordiales,

Abrir en Outlook

① Use la descarga .eml que aparece a continuación. Reemplace todos los **[marcadores de posición entre corchetes]** antes de enviar.

✉ Abrir Outlook (solo asunto)

⬇ Descargar plantilla .eml

Sherlock 2 - Resultado - No se observaron IoC (por archivo)

caso de uso

Enviado después de que el análisis técnico de administración no muestre indicadores de compromiso observados para un archivo cargado específico. Se envía una vez por archivo procesado.

Asunto

Actualización: Resultados del análisis de componentes de SD-WAN [insertar nombre del archivo] - CVE-2026-20182

Mensaje

Estimado cliente:

Gracias por su paciencia.

Hemos finalizado el análisis del archivo admin-tech [Insertar nombre de archivo]. En dicho archivo, no identificamos ningún indicador de compromiso relacionado con CVE-2026-20182 para este dispositivo específico.

Tenga en cuenta que la cantidad de datos de registro que recuperó y proporcionó a Cisco para esta revisión puede haber estado limitada por el período de retención de registro que configuró según la **Guía de Cisco SD-WAN Hardening^[1]**.

Importante: Pasos siguientes y cierre del caso:

1. **Esperar todos los resultados:** Tenga en cuenta que los resultados de este correo electrónico pueden ser parciales. Analizaremos cada archivo a medida que se proporcione. Espere hasta que reciba la confirmación de todos los archivos cargados antes de considerar que la evaluación ha finalizado.
2. **Prioridad de actualización:** Aunque los análisis preliminares de los registros de administración y tecnología no han identificado indicadores de compromiso (IoC), la vulnerabilidad subyacente puede permanecer. En el caso de las implementaciones de Cisco Cloud-Pro y Cisco On-Prem, si aún no lo ha hecho, dé prioridad a la actualización completa de los componentes de control de SD-WAN lo antes posible.
 - Nube de Cisco (fka: SaaS), los fabrics de los clientes son actualizados automáticamente por Cisco como parte del servicio gestionado. No es necesario realizar ninguna acción.
3. **Cierre del caso:** Una vez que haya recibido los resultados de "no se ha observado ningún IoC" para todos los archivos cargados Y (si procede) haya completado correctamente la actualización de software en su entorno, puede considerar que este caso se ha resuelto y continuar con los procedimientos de cierre estándar.

Actualizar recursos (si procede): Consulte el siguiente documento oficial de Cisco para obtener instrucciones detalladas sobre cómo realizar la actualización para Cisco Cloud-Pro y Cisco On-Prem: Guía de actualización de SD-WAN de Cisco

Una descripción general de alto nivel del proceso de actualización incluye:

1. Cargar las imágenes de software adecuadas en el repositorio de Manager (vManage).
2. Actualización secuencial de los controladores, empezando por Manager (vManage), seguido de Validator (vBond) y Controller (vSmart).
3. Activación de las nuevas versiones de software y validación de la funcionalidad del sistema.

Seguiremos supervisando su caso. Si no recibimos ninguna respuesta en un plazo de 10 días laborables tras haber proporcionado todos los resultados en función de los archivos que hemos recibido de usted, asumiremos que no se necesita más asistencia y procederemos con los procedimientos normales de cierre de casos del TAC. Si necesita

ayuda en algún momento, por favor háganoslo saber.

Saludos cordiales,

Abrir en Outlook

① Reemplazar todos los **[marcadores de posición entre corchetes]** antes de enviar.

✉ Abrir Outlook (solo asunto)

↓ Descargar plantilla .eml

Sherlock 3 - Recordatorio - Faltan archivos de Admin-Tech

caso de uso

Seguimiento automatizado cuando los archivos admin-tech enviados no coinciden con el número de componentes de control SD-WAN encontrados en los registros.

Asunto

Recuerde: Faltan archivos técnicos de administración necesarios para la evaluación de CVE-2026-20182

Mensaje

Estimado cliente:

Aún nos faltan técnicos de administración en los componentes de control de la SD-WAN, por lo que nuestro sistema no puede evaluar ningún indicador de compromiso a partir de los registros de la tecnología de administración. Para comenzar la evaluación de CVE-2026-20182, debemos recibir archivos de tecnología de administración de TODOS los controladores (vsmarts), validadores (vBonds) y administradores (vManage), incluidos todos los nodos de administrador (vManage) si están agrupados.

Pasos siguientes:

Cargue los archivos técnicos de administración restantes lo antes posible.

Saludos cordiales,

Abrir en Outlook

① Reemplazar todos los [marcadores de posición entre corchetes] antes de enviar.

✉ Abrir Outlook (con cuerpo)

↓ Descargar plantilla .eml

TAC 1 - Investigación - Se requiere una revisión adicional (se sospecha de IoC)

caso de uso

Enviado por un ingeniero del TAC una vez que la automatización ha encontrado registros que indican un posible riesgo y se requiere una investigación humana.

Asunto

Nº de SR: **se necesita más investigación**

Mensaje

Estimado cliente:

Mi nombre es {your_name} y he aceptado su caso. Gracias por su continua cooperación con el Centro de asistencia técnica de Cisco (TAC).

Tras un análisis preliminar de los archivos técnicos de administración que nos proporcionó de **sus componentes de control de SD-WAN**, hemos identificado que se requiere una investigación adicional del TAC para completar nuestro análisis. Para ayudar a garantizar una resolución completa y precisa, colaboraré estrechamente con usted en los siguientes pasos.

Tenga la seguridad de que nos comprometemos a apoyarle durante estos próximos pasos y le proporcionaremos una orientación clara para abordar la situación de forma eficaz.

Priorice la planificación y ejecución de actualizaciones como el paso más importante para mitigar este riesgo. Si aún no ha programado esta actualización, hágalo inmediatamente.

Si tiene alguna pregunta o necesita ayuda, no dude en ponerse en contacto con su ingeniero del TAC.

Gracias por su atención y colaboración.

Saludos cordiales,

Abrir en Outlook

① Reemplazar todos los [marcadores de posición entre corchetes] antes de enviar.

✉ Abrir Outlook (con cuerpo)

⬇ Descargar plantilla .eml

TAC 2 - Resultado - No se han encontrado loC (confirmado por el ingeniero)

caso de uso

Enviado por el ingeniero del TAC una vez que la automatización no ha encontrado ningún indicador de compromiso y el ingeniero ha confirmado el resultado.

Asunto

Actualización: Revisión del TAC finalizada: no se han encontrado loC para CVE-2026-20182 - Caso [SR #]

Mensaje

Hola, [Nombre del cliente]:

Soy el ingeniero del TAC de Cisco asignado a su caso [número de SR].

Después de realizar un análisis preliminar de los archivos técnicos de administración que proporcionó de los componentes de control de la SD-WAN, no encontramos entradas de registro coherentes con los indicadores de compromiso descritos en los avisos de seguridad de la SD-WAN de Cisco:

- **Vulnerabilidad de omisión de autenticación del controlador Cisco Catalyst SD-WAN [1]**
- **Vulnerabilidades de Cisco Catalyst SD-WAN Manager [2]**

Sin embargo, debe proceder a actualizar todos los componentes de control de SD-WAN a <insert version>. Estos son los pasos para continuar con la actualización:

- **Inicie la actualización de Catalyst SD-WAN [3]**
- **Guía de actualización para SD-WAN de Cisco[4]**

Tenga en cuenta que Cisco no puede evaluar los registros de los dispositivos periféricos debido a la naturaleza dinámica del direccionamiento IP en Internet y a nuestro desconocimiento de las direcciones IP esperadas de los dispositivos periféricos en la red de un cliente. Se recomienda a los clientes que sigan la Guía de validación de eventos de peering que se menciona en el Aviso de seguridad de omisión de autenticación del controlador SD-WAN de Cisco Catalyst para completar manualmente este paso. También se recomienda a los clientes que completen los pasos de detección adicionales relacionados con la validación de eventos de iguales, como se describe en el Aviso de seguridad para CVE-2026-20182.

Enlaces

[1] Vulnerabilidad de omisión de autenticación del controlador Cisco Catalyst SD-WAN:

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW>

[2] Vulnerabilidades de Cisco Catalyst SD-WAN Manager:

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-mltnps2-JxpWm7R>

[3] Inicie la actualización de la SD-WAN de Catalyst: <https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/225515-start-your-catalyst-sd-wan-upgrade.html>

[4] Guía de actualización de la SD-WAN de Cisco: <https://www.cisco.com/c/en/us/support/docs/wan/dpt/220424-upgrade-sd-wan-controllers-with-the-use.html>

Atentamente,

Abrir en Outlook

① Reemplazar todos los **[marcadores de posición entre corchetes]** antes de enviar.

✉ Abrir Outlook (solo asunto)

↓ Descargar plantilla .eml

TAC 3 - Validación - Confirmar propiedad de IP en superposición

caso de uso

Enviado por un ingeniero del TAC para preguntar al cliente si las direcciones IP específicas que aparecieron durante el análisis de registro son o eran parte de su infraestructura de superposición SD-WAN.

Asunto

[SR #] - Se requiere validación de dirección IP

Mensaje

Estimado/a [Nombre del cliente]:

Me llamo [Su nombre] y soy el ingeniero del TAC de Cisco asignado a su caso.

Como parte de nuestro análisis continuo de los archivos admin-tech que proporcionó de sus componentes de control SD-WAN, necesitamos su ayuda para validar si las siguientes direcciones IP son o fueron anteriormente parte de su infraestructura de superposición SD-WAN:

Direcciones IP en cuestión:

- [Dirección IP 1]
- [Dirección IP 2]

Para ayudarnos a completar la evaluación, confirme:

1. ¿Está asociada actualmente esta dirección IP a algún componente de la superposición SD-WAN (por ejemplo, vManage, vSmart, vBond o dispositivo periférico)?
2. ¿Alguna vez ha utilizado esta dirección IP algún componente de control de SD-WAN que se haya retirado del servicio o cuyo IP se haya cambiado?
3. ¿Está esta IP asociada a un sitio de recuperación ante desastres (DR) o a cualquier otra infraestructura relacionada con su implementación de SD-WAN?

Su rápida respuesta nos permitirá continuar con nuestro análisis y le proporcionará los siguientes pasos adecuados.

Si tiene alguna pregunta, no dude en ponerse en contacto con nosotros.

Saludos cordiales,

Abrir en Outlook

① Reemplazar todos los [marcadores de posición entre corchetes] antes de enviar.

✉ Abrir Outlook (con cuerpo)

⬇ Descargar plantilla .eml

TAC 4 - Resultado - Falsos positivos borrados

caso de uso

Enviado por un ingeniero del TAC después de una revisión manual determina que el IoC inicial marcado por el análisis automatizado era un falso positivo.

Asunto

Actualización: Informe técnico sobre CVE-2026-20182 - Caso [número de caso]

Mensaje

Estimado cliente:

Gracias por su paciencia mientras nuestro equipo de ingeniería llevó a cabo una revisión manual de los archivos admin-tech que proporcionó de sus componentes de control SD-WAN.

Tras una investigación exhaustiva, hemos determinado que el indicador inicial de compromiso (IoC) marcado por nuestro proceso de análisis automatizado era un falso positivo, es decir, nuestra evaluación es que los IoC no son válidos.

Importante: Aunque se ha borrado esta alerta específica, tenga en cuenta que la vulnerabilidad asociada a [CVE-2026-20182](#)^[1] requiere una actualización de software para ayudar a garantizar la seguridad e integridad a largo plazo de su fabric SD-WAN.

Si aún no ha completado la actualización: Priorice la actualización completa de sus componentes de control SD-WAN tan pronto como sea posible. La actualización es la única forma de remediar esta vulnerabilidad de forma eficaz. Consulte la [Guía de actualización de la SD-WAN de Cisco](#)^[2] para obtener instrucciones detalladas.

Si ya ha completado la actualización: Puesto que hemos confirmado este hallazgo como un falso positivo y ya ha realizado la remediación del software, no es necesario realizar ninguna otra acción. Puede considerar que este caso se ha resuelto y continuar con los procedimientos de cierre estándar.

Agradecemos su diligencia a la hora de dar prioridad a la seguridad de su infraestructura. Si tiene alguna otra pregunta o necesita más ayuda, no dude en ponerse en contacto con nosotros.

Saludos cordiales,

Centro de la asistencia técnica de Cisco (TAC)

Enlaces:

[1] [Aviso oficial de seguridad](#)

[2] [Guía de actualización de SD-WAN de Cisco](#)

Abrir en Outlook

① Reemplazar todos los *[marcadores de posición entre corchetes]* antes de enviar.

✉ Abrir Outlook (solo asunto)

↓ Descargar plantilla .eml

TAC 5 - Crítico - IoC identificado, llamada de revisión de programación

caso de uso

Enviado por un ingeniero del TAC cuando se han confirmado posibles indicadores de compromiso y se requiere una llamada urgente del cliente para hablar de las conclusiones y los siguientes pasos.

Asunto

URGENTE: Resultados del análisis para CVE-2026-20182 - Indicador de compromiso identificado

Mensaje

Estimado cliente:

Gracias por su paciencia mientras analizamos los archivos admin-tech proporcionados para sus componentes de control SD-WAN.

Tras nuestra revisión técnica, hemos identificado posibles indicadores de compromiso (IoC) relacionados con CVE-2026-20182.

Dada la naturaleza de estos hallazgos, es fundamental que discutamos los detalles técnicos y los siguientes pasos recomendados tan pronto como sea posible. Nos gustaría programar una llamada con su equipo para revisar las conclusiones específicas y analizar la solución adecuada.

Pasos siguientes:

- **Programar una reunión:** Háganos saber si está disponible para realizar una breve llamada en las próximas [p. ej., de 4 a 8 horas] con el fin de revisar estos resultados.
- **Actualizar los componentes de control de SDWAN:** Actualice el administrador, controlador y validador de SDWAN a una versión fija lo antes posible.

Nuestro objetivo principal es ayudarle a proteger su entorno y a mitigar cualquier riesgo potencial. Agradecemos su pronta atención a este asunto y esperamos poder coordinarnos con usted.

Saludos cordiales,

Abrir en Outlook

① Reemplazar todos los *[marcadores de posición entre corchetes]* antes de enviar.

✉ Abrir Outlook (con cuerpo)

⬇ Descargar plantilla .eml

TAC 6 - Resultado - IoC duplicado (Cerrar y redirigir)

caso de uso

Enviado por un ingeniero del TAC cuando el análisis de IoC confirma conclusiones que coinciden con una SR anterior para el mismo cliente/entorno. El caso actual está cerrado y el cliente se redirige a la SR original, donde ya se ha proporcionado la guía de solución de problemas.

Asunto

Actualización: Revisión técnica de CVE-2026-20182 - Caso [N.º de SR] (IoC duplicado confirmado)

Mensaje

Estimado cliente:

Gracias por su paciencia mientras analizamos los archivos admin-tech proporcionados para sus componentes de control SD-WAN. Hemos determinado que los indicadores iniciales de compromiso (IoC) marcados por nuestro proceso de análisis son los mismos que los ya comunicados en **[Original SR #]**. Como se ha mencionado anteriormente, se recomienda una actualización urgente y continuar con una de las dos rutas de remediación descritas en la [Guía de remediación de TAC](#)^[2] para proteger su entorno lo antes posible. Consulte el [aviso oficial de seguridad para CVE-2026-20182](#)^[1] para obtener más información.

Procederé ahora a cerrar este caso. Utilice **[N.º de SR original]** para solicitar más orientación o asistencia técnica en relación con la actualización o la remediación.

Saludos cordiales,

[Su nombre]

Enlaces:

[1] [Aviso oficial de seguridad](#)

[2] [Guía de remediación del TAC](#)

Abrir en Outlook

① Reemplazar todos los **[marcadores de posición entre corchetes]** antes de enviar.

✉ Abrir Outlook (con cuerpo)

⬇ Descargar plantilla .eml

TAC 7 - Remediación - Seguimiento de opciones (después de la llamada)

caso de uso

Enviado después de la llamada de revisión de IoC para recapitular las rutas de remediación descritas. El cliente elige la opción A (Reimplementación con reinicio continuo), la opción B (Reimplementación con transición directa) o la opción C (reconstrucción completa del sistema).

Asunto

Seguimiento: Opciones de corrección para CVE-2026-20182

Mensaje

Estimado cliente:

Gracias por el tiempo que ha dedicado a analizar los resultados de nuestro reciente análisis. Como hemos comentado en la llamada anterior, le recomendamos que siga con una de las siguientes rutas de remediación para proteger su entorno.

Opción A: Reimplementación con reinicio continuo. Da prioridad a la continuidad operativa al evitar el tiempo de inactividad de la red, aunque conlleva un riesgo residual de persistencia de amenazas durante el proceso de transición.

Descripción: Implica la reimplementación del controlador, además de la rotación de claves SSH y certificados. Los componentes de controlador existentes se conectan durante la migración a través de vManage para implementar el nuevo fabric y, a continuación, se eliminan en cuanto se migra el dispositivo.

Opción B: Reimplementación con transición directa. Proporciona un mayor nivel de garantía de seguridad. Dado que los nuevos controladores nunca se conectan a los antiguos, existe un aislamiento total. Debido a esto, las operaciones de red en general se ven afectadas, ya que todos los dispositivos necesitan restablecer la conectividad e intercambiar información de ruta/conectividad. El tiempo de interrupción dependerá del número de sitios, el número de prefijos intercambiados, etc.

Descripción: Implica la reimplementación del controlador más la rotación de claves SSH y certificados, pero los componentes del controlador antiguo se aíslan del nuevo fabric durante la reimplementación.

Opción C: Reconstruir todo el sistema. Proporciona el nivel más alto de garantía de seguridad al establecer una línea de base limpia, aunque es el enfoque más complejo y conlleva un mayor riesgo de inestabilidad relacionada con la configuración durante la reconstrucción. Se trata de una opción larga que requiere experiencia en la reconstrucción de las bases de datos de plantillas y políticas.

Pasos siguientes:

- Analice estas opciones internamente y díganos qué camino tiene previsto tomar. Una vez que lo haya decidido, podemos ofrecerle más orientación o asistencia técnica para ayudarle durante la fase de ejecución.

Estamos aquí para apoyarle durante todo este proceso. Háganos saber si tiene alguna pregunta relacionada con estas opciones.

Saludos cordiales,

Centro de la asistencia técnica de Cisco (TAC)

NOTE: La opción 1 fue la actualización. El escenario considerado para esta actualización ya se ha realizado.

Abrir en Outlook

① Use la descarga .eml que aparece a continuación. Reemplace todos los **[marcadores de posición entre corchetes]** antes de

enviar.

✉ Abrir Outlook (solo asunto)

↓ Descargar plantilla .eml

TAC 8 - Remediación - Opciones actualizadas para estructuras en riesgo (Opción 2 Seguimiento)

caso de uso

Notificar a los clientes cuyos fabrics SD-WAN se han visto comprometidos y perseguido anteriormente la opción 2 y cuyos fabrics se cree que siguen estando en riesgo de persistencia de los agentes de amenazas. Los clientes que han reconstruido su fabric comprometido (y no han confiado en una configDB de copia de seguridad/existente) no se suponen en riesgo y no recibirán esta comunicación. Esta comunicación será enviada por TBD.

Asunto

Acción urgente requerida: Solución de vulnerabilidades críticas de la infraestructura SD-WAN

Mensaje

Estimado cliente:

Proporcionamos una actualización crítica para la remediación de su fabric SD-WAN, como se indica en [SR#] y en los avisos de seguridad previamente comunicados. Esta actualización es específica para aquellos fabrics en los que los registros proporcionados mostraron evidencia de indicadores de compromiso (IOC).

Aunque anteriormente seleccionó un plan de remediación basado en la opción 2 (que incorpora una actualización de software, una reimplementación del controlador y la rotación de claves SSH), nuestro análisis del panorama de amenazas ha seguido evolucionando. Las nuevas perspectivas técnicas sobre la explotación de estas vulnerabilidades indican que se insta encarecidamente a adoptar medidas adicionales para reducir el riesgo de persistencia y ayudar a garantizar la integridad de la cadena de confianza de certificados.

Acción requerida:

Hemos actualizado las estrategias de remediación recomendadas para proporcionar una defensa más completa mediante la inclusión de la rotación adicional de certificados raíz.

Tenga en cuenta que las soluciones requerirán actividades de mantenimiento adicionales, que pueden incluir el tiempo de inactividad de la red planificado.

Dado que nuestra prioridad es la seguridad y la integridad de su red, hemos desarrollado tres opciones de remediación distintas. Cada una de las siguientes opciones proporciona un equilibrio entre el impacto operativo y la garantía de seguridad que debe tener en cuenta. Como su postura ante los riesgos internos es única, Cisco no puede recomendar una ruta concreta.

Opción A: Reimplementación con reinicio continuo. Da prioridad a la continuidad operativa al evitar el tiempo de inactividad de la red, aunque conlleva un riesgo residual de persistencia de amenazas durante el proceso de transición.

Descripción: Implica la reimplementación del controlador, además de la rotación de claves SSH y certificados. Los componentes de controlador existentes se conectan durante la migración a través de vManage para implementar el nuevo fabric y, a continuación, se eliminan en cuanto se migra el dispositivo.

Opción B: Reimplementación con transición directa. Proporciona un mayor nivel de garantía de seguridad. Dado que los nuevos controladores nunca se conectan a los antiguos, existe un aislamiento total. Debido a esto, las operaciones de red en general se ven afectadas, ya que todos los dispositivos necesitan restablecer la conectividad e intercambiar información de ruta/conectividad. El tiempo de interrupción dependerá del número de sitios, el número de prefijos intercambiados, etc.

Descripción: Implica la reimplementación del controlador más la rotación de claves SSH y certificados, pero los componentes del controlador antiguo se aíslan del nuevo fabric durante la reimplementación.

Opción C: Reconstruir todo el sistema. Proporciona el nivel más alto de garantía de seguridad al establecer una línea de base limpia, aunque es el enfoque más complejo y conlleva un mayor riesgo de inestabilidad relacionada con la configuración durante la reconstrucción. Se trata de una opción larga que requiere experiencia en la reconstrucción de las bases de datos de plantillas y políticas.

Una vez que su equipo haya revisado estas opciones y haya identificado el enfoque que mejor se adapte a sus estándares de gestión de riesgos, háganoslo saber respondiendo a este mensaje. Al recibir su selección, coordinaremos la ventana de mantenimiento y comenzaremos los preparativos técnicos necesarios para la ejecución.

Agradecemos que siga centrándose en mantener una infraestructura de red segura. Si necesita más información técnica, póngase en contacto con nosotros abriendo una solicitud de servicio (SR) con nuestro centro de asistencia técnica (TAC).

Atentamente,
Cisco

Abrir en Outlook

① Use la descarga .eml que aparece a continuación. Reemplace todos los **[marcadores de posición entre corchetes]** antes de enviar.

✉ Abrir Outlook (solo asunto)

↓ Descargar plantilla .eml

TAC 17: hallazgo inverso. Anteriormente sin IoC, ahora IoC identificado (CVE-2026-20182)

caso de uso

Enviado a clientes a los que se **había informado previamente de que no se** habían encontrado **indicadores de compromiso (IoC)**, pero para los que una **revisión interna posterior** de los registros de administración y tecnología ha **identificado** desde entonces los **IoC** relacionados con CVE-2026-20182. Comunica la conclusión revisada y proporciona las tres opciones de remediación (opción A, B o C).

Asunto

Actualización importante: Evaluación de IoC revisada para CVE-2026-20182 - Indicadores de compromiso ahora identificados - SR [SR#]

Mensaje

Estimado cliente:

Gracias por su continua cooperación con el centro de asistencia técnica Cisco Technical Assistance Center (TAC) con respecto a CVE-2026-20182 en la solicitud de servicio [SR#].

En nuestra correspondencia anterior, le informamos de que nuestro análisis de los archivos técnicos de administración proporcionados por los componentes de control de la SD-WAN no identificaba ningún indicador de compromiso (IoC) relacionado con este aviso. Como parte de nuestro compromiso continuo con su seguridad, desde entonces hemos llevado a cabo una revisión interna rutinaria de los datos de registro de administración y tecnología asociados con el fabric de su organización.

Este examen posterior ha identificado indicadores de compromiso (IoC) que no aparecieron durante la evaluación inicial. Ahora estamos trabajando con usted para abordar estas conclusiones. Estos IoC indican actividades potencialmente sospechosas dentro del fabric de su organización que justifican acciones de remediación.

Reconocemos que esto revisa los resultados que se le comunicaron previamente y queremos asegurarnos de que tiene una imagen clara y precisa de su entorno para que se pueda tomar la solución adecuada.

Acción requerida:

Tenga en cuenta que las soluciones requerirán actividades de mantenimiento adicionales, que pueden incluir el tiempo de inactividad de la red planificado.

Dado que nuestra prioridad es la seguridad y la integridad de su red, hemos desarrollado tres opciones de remediación distintas. Cada una de las siguientes opciones proporciona un equilibrio entre el impacto operativo y la garantía de seguridad que debe tener en cuenta. Como su postura ante los riesgos internos es única, Cisco no puede recomendar una ruta concreta.

Opción A: Reimplementación con reinicio continuo. Da prioridad a la continuidad operativa al evitar el tiempo de inactividad de la red, aunque conlleva un riesgo residual de persistencia de amenazas durante el proceso de transición.

Descripción: Implica la reimplementación del controlador, además de la rotación de claves SSH y certificados. Los componentes de controlador existentes se conectan durante la migración a través de vManage para implementar el

nuevo fabric y, a continuación, se eliminan en cuanto se migra el dispositivo.

Opción B: Reimplementación con transición directa. Proporciona un mayor nivel de garantía de seguridad. Dado que los nuevos controladores nunca se conectan a los antiguos, existe un aislamiento total. Debido a esto, las operaciones de red en general se ven afectadas, ya que todos los dispositivos necesitan restablecer la conectividad e intercambiar información de ruta/conectividad. El tiempo de interrupción dependerá del número de sitios, el número de prefijos intercambiados, etc.

Descripción: Implica la reimplementación del controlador más la rotación de claves SSH y certificados, pero los componentes del controlador antiguo se aíslan del nuevo fabric durante la reimplementación.

Opción C: Reconstruir todo el sistema. Proporciona el nivel más alto de garantía de seguridad al establecer una línea de base limpia, aunque es el enfoque más complejo y conlleva un mayor riesgo de inestabilidad relacionada con la configuración durante la reconstrucción. Se trata de una opción larga que requiere experiencia en la reconstrucción de las bases de datos de plantillas y políticas.

Una vez que su equipo haya revisado estas opciones y haya identificado el enfoque que mejor se adapte a sus estándares de gestión de riesgos, háganoslo saber respondiendo a este mensaje. Al recibir su selección, coordinaremos la ventana de mantenimiento y comenzaremos los preparativos técnicos necesarios para la ejecución.

Agradecemos que siga centrándose en mantener una infraestructura de red segura. Por favor, háganos saber si necesita más aclaraciones técnicas respondiendo a este correo electrónico o a través de la Solicitud de servicio (SR) existente con nuestro Centro de asistencia técnica (TAC).

Atentamente,
Cisco

Abrir en Outlook

① Use la descarga .eml que aparece a continuación. Reemplace todos los **[marcadores de posición entre corchetes]** antes de enviar.

✉ Abrir Outlook (solo asunto)

↓ Descargar plantilla .eml

CloudOps 1 - Proactivo - IoC detectado en Cloud Scan, se requiere tecnología administrativa para validar

caso de uso

Se envía de forma proactiva cuando un análisis de seguridad de Cisco CloudOps de un fabric SD-WAN alojado en la nube ha revelado posibles indicadores de compromiso (IoC). Se abre una SR en nombre del cliente y se le pide que adjunte archivos de administración y tecnología para poder validar los resultados mediante un análisis de registro completo.

Asunto

Acción requerida: Archivos técnicos de administración necesarios para validar las conclusiones del análisis de seguridad - SR [SR#]

Mensaje

Estimado cliente:

Como parte de nuestro compromiso continuo de proteger y supervisar la integridad de las ofertas de Cisco, Cisco ha completado recientemente un análisis de seguridad de determinados fabricas SD-WAN alojados en la nube. Esta medida se adoptó en respuesta a un problema de seguridad notificado. El análisis ha identificado actividad potencialmente sospechosa en el fabric de su organización que merece una revisión más a fondo.

Solicitamos su ayuda para adjuntar archivos de administración y tecnología a esta solicitud de servicio (SR), que se abrió en su nombre, para que podamos validar esta conclusión y completar nuestra investigación.

Para habilitar un análisis completo, recopile y cargue los archivos admin-tech de todos los componentes de control de SD-WAN. Asegúrese de seleccionar **"Registros"** y **"Tecnología"** al generar estos archivos:

- **vsmarts (controladores):** Recopile uno a la vez, no simultáneamente.
- **vBonds (validadores):** Recopilar de todos los nodos.
- **Administrador (vManage):** Recopile datos de todos los nodos del clúster (DR activo y en espera).

Para obtener instrucciones detalladas paso a paso sobre cómo generar y enviar de forma segura sus archivos admin-tech, consulte esta guía: [Guía de recopilación de tecnología de administración de Cisco SD-WAN](#)^[1].

Una vez que recibamos los archivos solicitados, nuestro equipo los analizará para confirmar si la actividad observada representa un auténtico indicador de compromiso y le aconsejará sobre los siguientes pasos adecuados.

Agradecemos que siga centrándose en mantener una infraestructura de red segura. Háganos saber si necesita más información técnica respondiendo a esta solicitud de servicio (SR).

Saludos cordiales,

Cisco

Enlaces:

[1] [Guía de recopilación de tecnología de administración de Cisco SD-WAN](#)

Abrir en Outlook

① Use la descarga .eml que aparece a continuación. Reemplace todos los **[marcadores de posición entre corchetes]** antes de enviar.

✉ Abrir Outlook (solo asunto)

↓ Descargar plantilla .eml

Mensajes de correo electrónico para WAVE 2A para clientes que SUFRIERON UN IMPACTO ANTERIOR y que aún no han completado las opciones A, B o C. (Las opciones 1 y 2 deben rehacerse)

Plantilla de TAC 9 para sin IOC para PSIRT2a/se reconstruyeron (**IMPACTADO PREVIAMENTE**)

caso de uso

Enviados a clientes cuyos registros de SD-WAN **no** mostraban **indicadores de compromiso (IoC)** relacionados con el asesor PSIRT2a Y que **habían reconstruido previamente** su fabric. Proporciona directrices de corrección actualizadas con tres opciones (opción 2, seguimiento).

Asunto

Acción urgente requerida: Solución de vulnerabilidades críticas de la infraestructura SD-WAN - SR [SR#]

Mensaje

Estimado cliente:

Gracias por ponerse en contacto con el centro de asistencia técnica Cisco Technical Assistance Center (TAC) con respecto a los últimos avisos PSIRT para SD-WAN de la solicitud de servicio [SR#].

Después de revisar los registros y la información proporcionada desde su fabric de SD-WAN, nuestro análisis no identificó ningún indicador de compromiso (IOC) asociado con el aviso de vulnerabilidad de SD-WAN del 5 de junio de 2026. Además, entendemos que su entorno se ha reconstruido anteriormente como parte de los esfuerzos de remediación relacionados con las recomendaciones anteriores.

Nos gustaría compartir una importante actualización con respecto a la guía de remediación recomendada para fabrics SD-WAN teniendo en cuenta las nuevas perspectivas identificadas relacionadas con estas vulnerabilidades.

Proporcionamos una actualización crítica para la remediación de su fabric SD-WAN, como se indica en [SR#] y en los avisos de seguridad previamente comunicados.

Aunque anteriormente seleccionó un plan de remediación basado en la opción 2 (que incorpora una actualización de software, una reimplementación del controlador y la rotación de claves SSH), nuestro análisis del panorama de amenazas ha seguido evolucionando. Las nuevas perspectivas técnicas sobre la explotación de estas vulnerabilidades indican que se insta encarecidamente a adoptar medidas adicionales para reducir el riesgo de persistencia y ayudar a garantizar la integridad de la cadena de confianza de certificados.

Acción requerida:

Hemos actualizado las estrategias de remediación recomendadas para proporcionar una defensa más completa mediante la inclusión de la rotación adicional de certificados raíz.

Tenga en cuenta que las soluciones requerirán actividades de mantenimiento adicionales, que pueden incluir el tiempo de inactividad de la red planificado. Dado que nuestra prioridad es la seguridad y la integridad de su red, hemos desarrollado tres opciones de remediación distintas. Cada una de las siguientes opciones proporciona un equilibrio entre el impacto operativo y la garantía de seguridad que debe tener en cuenta. Como su postura ante los riesgos internos es única, Cisco no puede recomendar una ruta concreta.

Opción A: Reimplementación con reinicio continuo. Da prioridad a la continuidad operativa al evitar el tiempo de inactividad de la red, aunque conlleva un riesgo residual de persistencia de amenazas durante el proceso de transición.

Descripción: Implica la reimplementación del controlador, además de la rotación de claves SSH y certificados. Los componentes de controlador existentes se conectan durante la migración a través de vManage para implementar el nuevo fabric y, a continuación, se eliminan en cuanto se migra el dispositivo.

Opción B: Reimplementación con transición directa. Proporciona un mayor nivel de garantía de seguridad. Dado que los nuevos controladores nunca se conectan a los antiguos, existe un aislamiento total. Debido a esto, las operaciones de red en general se ven afectadas, ya que todos los dispositivos necesitan restablecer la conectividad e intercambiar información de ruta/conectividad. El tiempo de interrupción dependerá del número de sitios, el número de prefijos intercambiados, etc.

Descripción: Implica la reimplementación del controlador más la rotación de claves SSH y certificados, pero los componentes del controlador antiguo se aíslan del nuevo fabric durante la reimplementación.

Opción C: Reconstruir todo el sistema. Proporciona el nivel más alto de garantía de seguridad al establecer una línea de base limpia, aunque es el enfoque más complejo y conlleva un mayor riesgo de inestabilidad relacionada con la configuración durante la reconstrucción. Se trata de una opción larga que requiere experiencia en la reconstrucción de las bases de datos de plantillas y políticas.

Una vez que su equipo haya revisado estas opciones y haya identificado el enfoque que mejor se adapte a sus estándares de gestión de riesgos, háganoslo saber respondiendo a este mensaje. Al recibir su selección, coordinaremos la ventana de mantenimiento y comenzaremos los preparativos técnicos necesarios para la ejecución.

Agradecemos que siga centrándose en mantener una infraestructura de red segura. Por favor, háganos saber si necesita más aclaraciones técnicas respondiendo a este correo electrónico o a través de la Solicitud de servicio existente.

Atentamente,

Cisco

Abrir en Outlook

① Use la descarga .eml que aparece a continuación. Reemplace todos los **[marcadores de posición entre corchetes]** antes de enviar.

✉ Abrir Outlook (solo asunto)

↓ Descargar plantilla .eml

Plantilla de TAC 10 para sí IOC para PSIRT2a/se reconstruyeron (**IMPACTADO PREVIAMENTE**)

caso de uso

Enviados a clientes cuyos registros de SD-WAN mostraban **indicadores de compromiso (IoC)** relacionados con el asesoramiento de PSIRT2a Y que **habían reconstruido** su fabric con **anterioridad**. Proporciona directrices de corrección actualizadas con tres opciones (opción 2, seguimiento).

Asunto

Acción urgente requerida: Solución de vulnerabilidades críticas de la infraestructura SD-WAN - SR [SR#]

Mensaje

Estimado cliente:

Gracias por ponerse en contacto con el centro de asistencia técnica Cisco Technical Assistance Center (TAC) con respecto a los últimos avisos PSIRT para SD-WAN de la solicitud de servicio [SR#].

Después de analizar los registros proporcionados desde su fabric de SD-WAN, nuestro equipo ha identificado los indicadores de compromiso (IOC) asociados con el aviso de vulnerabilidad de SD-WAN del 5 de junio de 2026. También entendemos que su entorno se ha reconstruido anteriormente como parte de los pasos de remediación relacionados con las recomendaciones anteriores.

Proporcionamos una actualización crítica para la remediación de su fabric SD-WAN, como se indica en [SR#] y en los avisos de seguridad previamente comunicados. Esta actualización es específica para aquellos fabrics en los que los registros proporcionados mostraron evidencia de indicadores de compromiso (IOC).

Aunque anteriormente seleccionó un plan de remediación basado en la opción 2 (que incorpora una actualización de software, una reimplementación del controlador y la rotación de claves SSH), nuestro análisis del panorama de amenazas ha seguido evolucionando. Las nuevas perspectivas técnicas sobre la explotación de estas vulnerabilidades indican que se insta encarecidamente a adoptar medidas adicionales para reducir el riesgo de persistencia y ayudar a garantizar la integridad de la cadena de confianza de certificados.

Acción requerida:

Hemos actualizado las estrategias de remediación recomendadas para proporcionar una defensa más completa

mediante la inclusión de la rotación adicional de certificados raíz.

Tenga en cuenta que las soluciones requerirán actividades de mantenimiento adicionales, que pueden incluir el tiempo de inactividad de la red planificado. Dado que nuestra prioridad es la seguridad y la integridad de su red, hemos desarrollado tres opciones de remediación distintas. Cada una de las siguientes opciones proporciona un equilibrio entre el impacto operativo y la garantía de seguridad que debe tener en cuenta. Como su postura ante los riesgos internos es única, Cisco no puede recomendar una ruta concreta.

Opción A: Reimplementación con reinicio continuo. Da prioridad a la continuidad operativa al evitar el tiempo de inactividad de la red, aunque conlleva un riesgo residual de persistencia de amenazas durante el proceso de transición.

Descripción: Implica la reimplementación del controlador, además de la rotación de claves SSH y certificados. Los componentes de controlador existentes se conectan durante la migración a través de vManage para implementar el nuevo fabric y, a continuación, se eliminan en cuanto se migra el dispositivo.

Opción B: Reimplementación con transición directa. Proporciona un mayor nivel de garantía de seguridad. Dado que los nuevos controladores nunca se conectan a los antiguos, existe un aislamiento total. Debido a esto, las operaciones de red en general se ven afectadas, ya que todos los dispositivos necesitan restablecer la conectividad e intercambiar información de ruta/conectividad. El tiempo de interrupción dependerá del número de sitios, el número de prefijos intercambiados, etc.

Descripción: Implica la reimplementación del controlador más la rotación de claves SSH y certificados, pero los componentes del controlador antiguo se aíslan del nuevo fabric durante la reimplementación.

Opción C: Reconstruir todo el sistema. Proporciona el nivel más alto de garantía de seguridad al establecer una línea de base limpia, aunque es el enfoque más complejo y conlleva un mayor riesgo de inestabilidad relacionada con la configuración durante la reconstrucción. Se trata de una opción larga que requiere experiencia en la reconstrucción de las bases de datos de plantillas y políticas.

Una vez que su equipo haya revisado estas opciones y haya identificado el enfoque que mejor se adapte a sus estándares de gestión de riesgos, háganoslo saber respondiendo a este mensaje. Al recibir su selección, coordinaremos la ventana de mantenimiento y comenzaremos los preparativos técnicos necesarios para la ejecución.

Agradecemos que siga centrándose en mantener una infraestructura de red segura. Por favor, háganos saber si necesita más aclaraciones técnicas respondiendo a este correo electrónico o a través de la Solicitud de servicio existente.

Atentamente,
Cisco

① Use la descarga .eml que aparece a continuación. Reemplace todos los **[marcadores de posición entre corchetes]** antes de enviar.

✉ Abrir Outlook (solo asunto)

↓ Descargar plantilla .eml

Plantilla TAC 11 para sin IOC para PSIRT2a/no se reconstruyeron (**IMPACTADO PREVIAMENTE**)

caso de uso

Enviados a clientes cuyos registros de SD-WAN **no** mostraban **indicadores de compromiso (IoC)** relacionados con el asesoramiento de PSIRT2a Y que **NO reconstruyeron** su fabric. Proporciona directrices de corrección actualizadas con tres opciones (opción 1 de seguimiento).

Asunto

Acción urgente requerida: Solución de vulnerabilidades críticas de la infraestructura SD-WAN - SR [SR#]

Mensaje

Estimado cliente:

Gracias por ponerse en contacto con el centro de asistencia técnica Cisco Technical Assistance Center (TAC) con respecto a los últimos avisos PSIRT para SD-WAN de la solicitud de servicio [SR#].

Después de revisar los registros y la información proporcionada desde su fabric de SD-WAN, no identificamos los indicadores de compromiso (IOC) asociados con el aviso de vulnerabilidad de SD-WAN del 5 de junio de 2026.

También entendemos que su entorno no ha sido objeto de una reconstrucción completa tras las recomendaciones anteriores. Cisco recomienda revisar la guía de remediación actualizada a continuación para ayudar a reducir la exposición potencial y fortalecer la integridad de la cadena de confianza del certificado SD-WAN.

Teniendo esto en cuenta, estamos proporcionando una actualización crítica para la remediación de su fabric SD-WAN, como se indica en [SR#] y en los avisos de seguridad previamente comunicados.

Aunque anteriormente seleccionó un plan de remediación basado en la opción 1 (que incorpora una actualización de software y rotación de claves SSH), nuestro análisis del panorama de amenazas ha seguido evolucionando. Las nuevas perspectivas técnicas sobre la explotación de estas vulnerabilidades indican que se insta encarecidamente a adoptar medidas adicionales para reducir el riesgo de persistencia y ayudar a garantizar la integridad de la cadena de confianza de certificados.

Acción requerida:

Hemos actualizado las estrategias de remediación recomendadas para proporcionar una defensa más completa

mediante la inclusión de la rotación adicional de certificados raíz.

Tenga en cuenta que las soluciones requerirán actividades de mantenimiento adicionales, que pueden incluir el tiempo de inactividad de la red planificado. Dado que nuestra prioridad es la seguridad y la integridad de su red, hemos desarrollado tres opciones de remediación distintas. Cada una de las siguientes opciones proporciona un equilibrio entre el impacto operativo y la garantía de seguridad que debe tener en cuenta. Como su postura ante los riesgos internos es única, Cisco no puede recomendar una ruta concreta.

Opción A: Reimplementación con reinicio continuo. Da prioridad a la continuidad operativa al evitar el tiempo de inactividad de la red, aunque conlleva un riesgo residual de persistencia de amenazas durante el proceso de transición.

Descripción: Implica la reimplementación del controlador, además de la rotación de claves SSH y certificados. Los componentes de controlador existentes se conectan durante la migración a través de vManage para implementar el nuevo fabric y, a continuación, se eliminan en cuanto se migra el dispositivo.

Opción B: Reimplementación con transición directa. Proporciona un mayor nivel de garantía de seguridad. Dado que los nuevos controladores nunca se conectan a los antiguos, existe un aislamiento total. Debido a esto, las operaciones de red en general se ven afectadas, ya que todos los dispositivos necesitan restablecer la conectividad e intercambiar información de ruta/conectividad. El tiempo de interrupción dependerá del número de sitios, el número de prefijos intercambiados, etc.

Descripción: Implica la reimplementación del controlador más la rotación de claves SSH y certificados, pero los componentes del controlador antiguo se aíslan del nuevo fabric durante la reimplementación.

Opción C: Reconstruir todo el sistema. Proporciona el nivel más alto de garantía de seguridad al establecer una línea de base limpia, aunque es el enfoque más complejo y conlleva un mayor riesgo de inestabilidad relacionada con la configuración durante la reconstrucción. Se trata de una opción larga que requiere experiencia en la reconstrucción de las bases de datos de plantillas y políticas.

Una vez que su equipo haya revisado estas opciones y haya identificado el enfoque que mejor se adapte a sus estándares de gestión de riesgos, háganoslo saber respondiendo a este mensaje. Al recibir su selección, coordinaremos la ventana de mantenimiento y comenzaremos los preparativos técnicos necesarios para la ejecución.

Agradecemos que siga centrándose en mantener una infraestructura de red segura. Por favor, háganos saber si necesita más aclaraciones técnicas respondiendo a este correo electrónico o a través de la Solicitud de servicio existente.

Atentamente,
Cisco

① Use la descarga .eml que aparece a continuación. Reemplace todos los **[marcadores de posición entre corchetes]** antes de enviar.

✉ Abrir Outlook (solo asunto)

↓ Descargar plantilla .eml

Plantilla TAC 12 para sí IOC para PSIRT2a/no se reconstruyeron (**IMPACTADO PREVIAMENTE**)

caso de uso

Enviados a clientes cuyos registros de SD-WAN mostraban **indicadores de compromiso (IOC)** relacionados con el asesoramiento de PSIRT2a Y que **NO reconstruyeron** su fabric. Proporciona directrices de corrección actualizadas con tres opciones (opción 1 de seguimiento).

Asunto

Acción urgente requerida: Solución de vulnerabilidades críticas de la infraestructura SD-WAN - SR [SR#]

Mensaje

Estimado cliente:

Gracias por ponerse en contacto con el centro de asistencia técnica Cisco Technical Assistance Center (TAC) con respecto a los últimos avisos PSIRT para SD-WAN de la solicitud de servicio [SR#].

Después de analizar los registros proporcionados desde su fabric de SD-WAN, nuestro equipo ha identificado los indicadores de compromiso (IOC) asociados con el aviso de vulnerabilidad de SD-WAN del 5 de junio de 2026. Además, entendemos que su entorno no se ha reconstruido completamente tras las recomendaciones anteriores.

Dada la presencia de estos indicadores y la comprensión en evolución del panorama de amenazas, es importante revisar e implementar la guía de remediación actualizada que se describe a continuación para reducir el riesgo de persistencia y garantizar la integridad de su cadena de confianza de certificados SD-WAN.

Proporcionamos una actualización crítica para la remediación de su fabric SD-WAN, como se indica en [SR#] y en los avisos de seguridad previamente comunicados. Esta actualización es específica para aquellos fabrics en los que los registros proporcionados mostraron evidencia de indicadores de compromiso (IOC).

Aunque anteriormente seleccionó un plan de remediación basado en la opción 1 (que incorpora una actualización de software y rotación de claves SSH), nuestro análisis del panorama de amenazas ha seguido evolucionando. Las nuevas perspectivas técnicas sobre la explotación de estas vulnerabilidades indican que se insta encarecidamente a adoptar medidas adicionales para reducir el riesgo de persistencia y ayudar a garantizar la integridad de la cadena de confianza de certificados.

Acción requerida:

Hemos actualizado las estrategias de remediación recomendadas para proporcionar una defensa más completa mediante la inclusión de la rotación adicional de certificados raíz.

Tenga en cuenta que las soluciones requerirán actividades de mantenimiento adicionales, que pueden incluir el tiempo de inactividad de la red planificado. Dado que nuestra prioridad es la seguridad y la integridad de su red, hemos desarrollado tres opciones de remediación distintas. Cada una de las siguientes opciones proporciona un equilibrio entre el impacto operativo y la garantía de seguridad que debe tener en cuenta. Como su postura ante los riesgos internos es única, Cisco no puede recomendar una ruta concreta.

Opción A: Reimplementación con reinicio continuo. Da prioridad a la continuidad operativa al evitar el tiempo de inactividad de la red, aunque conlleva un riesgo residual de persistencia de amenazas durante el proceso de transición.

Descripción: Implica la reimplementación del controlador, además de la rotación de claves SSH y certificados. Los componentes de controlador existentes se conectan durante la migración a través de vManage para implementar el nuevo fabric y, a continuación, se eliminan en cuanto se migra el dispositivo.

Opción B: Reimplementación con transición directa. Proporciona un mayor nivel de garantía de seguridad. Dado que los nuevos controladores nunca se conectan a los antiguos, existe un aislamiento total. Debido a esto, las operaciones de red en general se ven afectadas, ya que todos los dispositivos necesitan restablecer la conectividad e intercambiar información de ruta/conectividad. El tiempo de interrupción dependerá del número de sitios, el número de prefijos intercambiados, etc.

Descripción: Implica la reimplementación del controlador más la rotación de claves SSH y certificados, pero los componentes del controlador antiguo se aíslan del nuevo fabric durante la reimplementación.

Opción C: Reconstruir todo el sistema. Proporciona el nivel más alto de garantía de seguridad al establecer una línea de base limpia, aunque es el enfoque más complejo y conlleva un mayor riesgo de inestabilidad relacionada con la configuración durante la reconstrucción. Se trata de una opción larga que requiere experiencia en la reconstrucción de las bases de datos de plantillas y políticas.

Una vez que su equipo haya revisado estas opciones y haya identificado el enfoque que mejor se adapte a sus estándares de gestión de riesgos, háganoslo saber respondiendo a este mensaje. Al recibir su selección, coordinaremos la ventana de mantenimiento y comenzaremos los preparativos técnicos necesarios para la ejecución.

Agradecemos que siga centrándose en mantener una infraestructura de red segura. Por favor, háganos saber si necesita más aclaraciones técnicas respondiendo a este correo electrónico o a través de la Solicitud de servicio existente.

Atentamente,
Cisco

① Use la descarga .eml que aparece a continuación. Reemplace todos los **[marcadores de posición entre corchetes]** antes de enviar.

✉ Abrir Outlook (solo asunto)

↓ Descargar plantilla .eml

Correos electrónicos para WAVE 2A para nuevos clientes (no afectados anteriormente)

Plantilla TAC 13 para no IOC/versión fija no disponible (WAVE 2a — Await Fix)

caso de uso

Enviados a clientes cuyos registros de SD-WAN **no** mostraban **indicadores de compromiso (IoC)** relacionados con CVE-2026-20245, pero para los que **actualmente no hay ninguna versión de software fija disponible** para su plataforma/versión. Aconseja al cliente que aplique medidas de endurecimiento provisionales y espere a recibir la notificación de liberación fija.

Asunto

Actualización: Evaluación de IoC completada para CVE-2026-20245: versión fija no disponible actualmente; SR [SR#]

Mensaje

Estimado cliente:

Gracias por ponerse en contacto con el centro de asistencia técnica Cisco Technical Assistance Center (TAC) en relación con CVE-2026-20245 en la solicitud de servicio [SR#].

Hemos finalizado el análisis de los archivos de administración y tecnología que nos ha proporcionado de los componentes de control de la SD-WAN. **No identificamos ningún indicador de compromiso (IoC)** asociado con CVE-2026-20245 en los registros revisados.

Tenga en cuenta que la cantidad de datos de registro recuperados y proporcionados a Cisco para esta revisión puede haber estado limitada por el período de retención de registro configurado en su entorno de acuerdo con la [Guía de Cisco SD-WAN Hardening](#)^[1].

Importante: actualmente no hay ninguna versión de software fija disponible:

En este momento, **no hay ninguna versión de software fija disponible** para su plataforma y versión de software actuales para remediar esta vulnerabilidad. El departamento de ingeniería de Cisco trabaja activamente para ofrecer una versión fija. Una vez que el software fijo esté disponible, el [aviso oficial de seguridad](#)^[2] se actualizará con la información de versión fija.

Medidas provisionales recomendadas:

Mientras espera la versión fija, le recomendamos encarecidamente implementar las siguientes medidas de endurecimiento para reducir su exposición:

1. **Aplicar mejores prácticas de consolidación:** Revise e implemente las recomendaciones de la [Guía de endurecimiento de SD-WAN de Cisco](#)^[1] para reducir la superficie de ataque.
2. **Supervise el aviso de seguridad:** Consulte periódicamente el [aviso oficial de seguridad](#)^[2] [para ver si hay actualizaciones sobre la disponibilidad de versiones fijas para su plataforma](#).
3. **Plan de actualización:** Comience a planificar la actualización ahora para estar preparado para ejecutar la actualización rápidamente una vez que se publique la versión corregida.
4. **Supervise su entorno:** Continúe supervisando los componentes de control de SD-WAN para detectar cualquier comportamiento anómalo o cambio de configuración inesperado.

Pasos siguientes:

Actualizaremos este caso cuando la versión de software fija esté disponible. En ese momento, debe dar prioridad a la actualización de todos los componentes de control de SD-WAN (Manager, Controller, Validator) a la versión fija tan pronto como sea posible.

Si tiene una suscripción a BCS/LCS, póngase en contacto con su Cisco NCE o Delivery Manager para obtener orientación adicional sobre la planificación de actualizaciones.

Agradecemos su paciencia y su compromiso con la seguridad de su infraestructura. Si tiene alguna pregunta o necesita más ayuda mientras tanto, no dude en responder a este caso.

Saludos cordiales,

Centro de la asistencia técnica de Cisco (TAC)

Enlaces:

[1] [Guía de refuerzo de SD-WAN de Cisco](#)

[2] [Aviso de seguridad oficial \(cisco-sa-sdwan-privesc-4uxFrdzx\)](#)

Abrir en Outlook

① Reemplazar todos los **[marcadores de posición entre corchetes]** antes de enviar.

✉ Abrir Outlook (solo asunto)

↓ Descargar plantilla .eml

Plantilla de TAC 14 para versiones fijas o sin IOC disponibles (WAVE 2a — Actualice ahora)

caso de uso

Enviados a clientes cuyos registros de SD-WAN **no** mostraban **indicadores de compromiso (IoC)** relacionados con CVE-2026-20245 Y para los que **hay disponible** una **versión de software fija**. Aconseja al cliente que continúe con la planificación y ejecución de la actualización inmediatamente.

Asunto

Actualización: Evaluación de IoC completada para CVE-2026-20245 - No se encontraron IoC, se requiere actualización - SR [SR#]

Mensaje

Estimado cliente:

Gracias por ponerse en contacto con el centro de asistencia técnica Cisco Technical Assistance Center (TAC) en relación con CVE-2026-20245 en la solicitud de servicio [SR#].

Hemos finalizado el análisis de los archivos de administración y tecnología que nos ha proporcionado de los componentes de control de la SD-WAN. **No identificamos ningún indicador de compromiso (IoC)** asociado con CVE-2026-20245 en los registros revisados.

Tenga en cuenta que la cantidad de datos de registro recuperados y proporcionados a Cisco para esta revisión puede haber estado limitada por el período de retención de registro configurado en su entorno de acuerdo con la [Guía de Cisco SD-WAN Hardening](#)^[1].

Importante: actualización necesaria:

Aunque no se ha identificado ningún IoC, la vulnerabilidad subyacente permanece presente hasta que los componentes de control de la SD-WAN se actualicen a una versión de software fija. Ya hay disponible una versión fija para su plataforma.

Asigne **prioridad a la planificación y ejecución de actualizaciones** como el paso más importante para remediar esta vulnerabilidad. Si aún no ha programado esta actualización, hágalo inmediatamente.

Pasos siguientes:

1. **Actualizar todos los componentes de control de SD-WAN:** Actualice su Manager (vManage), Controller (vSmart) y Validator (vBond) a una versión de software fija enumerada en el [aviso de seguridad oficial](#)^[2].
2. **Recursos de actualización:** Consulte los siguientes documentos oficiales de Cisco para obtener instrucciones de actualización detalladas:
 - [Inicie la actualización de Catalyst SD-WAN](#)^[3]
 - [Guía de actualización para SD-WAN de Cisco](#)^[4]
3. **Cierre del caso:** Una vez que haya completado correctamente la actualización de software en su entorno, puede considerar que este caso se ha resuelto y continuar con los procedimientos de cierre estándar.

Si tiene una suscripción a BCS/LCS, póngase en contacto con su Cisco NCE o Delivery Manager para obtener orientación adicional sobre el proceso de actualización.

Seguiremos supervisando su caso. Si no recibimos la respuesta en un plazo de 10 días laborables, asumiremos que no se necesita más asistencia y procederemos con los procedimientos normales de cierre de casos del TAC.

Saludos cordiales,

Centro de la asistencia técnica de Cisco (TAC)

Enlaces:

[1] [Guía de refuerzo de SD-WAN de Cisco](#)

[2] [Aviso de seguridad oficial \(cisco-sa-sdwan-privesc-4uxFrzdx\)](#)

[3] [Inicie la actualización de Catalyst SD-WAN](#)

[4] [Guía de actualización de SD-WAN de Cisco](#)

Abrir en Outlook

① Reemplazar todos los **[marcadores de posición entre corchetes]** antes de enviar.

✉ Abrir Outlook (solo asunto)

⬇ Descargar plantilla .eml

Plantilla de TAC 15 para versiones de IOC identificadas/fijas disponibles (WAVE 2a — Actualización urgente)

caso de uso

Enviados a clientes cuyos registros de SD-WAN mostraban **indicadores de compromiso (IoC)** relacionados con CVE-2026-20245 Y para los que **hay disponible** una **versión de software fija**. Aconseja al cliente que actualice con urgencia y programe una llamada de revisión para hablar de las conclusiones y la remediación.

Asunto

URGENTE: IoC identificado para CVE-2026-20245 - Actualización inmediata necesaria - SR [SR#]

Mensaje

Estimado cliente:

Gracias por ponerse en contacto con el centro de asistencia técnica Cisco Technical Assistance Center (TAC) en relación con CVE-2026-20245 en la solicitud de servicio [SR#].

Después de analizar los archivos técnicos de administración proporcionados por los componentes de control de la SD-

WAN, nuestro equipo ha **identificado los indicadores de compromiso (IoC)** asociados con CVE-2026-20245.

Dada la naturaleza de estos hallazgos, es fundamental que discutamos los detalles técnicos y los siguientes pasos recomendados tan pronto como sea posible. Nos gustaría programar una llamada con su equipo para revisar las conclusiones específicas y analizar la ruta de solución adecuada.

Acciones inmediatas necesarias:

1. **Actualización inmediata de los componentes de control de SD-WAN:** Hay disponible una versión de software fija para su plataforma. Actualice su Manager (vManage), Controller (vSmart) y Validator (vBond) a una versión de software fija enumerada en el [aviso de seguridad oficial](#)^[1] lo antes posible. La actualización cierra la vulnerabilidad inmediatamente.
2. **Programar una llamada de revisión:** Háblenos de si está disponible para realizar una breve llamada en las próximas [p. ej., de 4 a 8 horas] con el fin de revisar las conclusiones de IoC y analizar las opciones de solución recomendadas.
3. **Aplicar mejores prácticas de consolidación:** Revise e implemente las recomendaciones de la [Guía de endurecimiento de SD-WAN de Cisco](#)^[2] para reducir la superficie de ataque mientras se planifica la remediación.

Recursos de actualización:

- [Inicie la actualización de Catalyst SD-WAN](#)^[3]
- [Guía de actualización para SD-WAN de Cisco](#)^[4]

Importante: Después de la actualización, se pueden recomendar pasos de corrección adicionales (como la reimplementación del controlador y la rotación de certificados) en función de la gravedad del riesgo identificado. Estos aspectos se tratarán durante la llamada de revisión.

Consulte también la [Guía de remediación del TAC](#)^[5] para ver opciones de remediación detalladas.

Nuestro objetivo principal es ayudarle a proteger su entorno y a mitigar cualquier riesgo potencial. Agradecemos su pronta atención a este asunto y esperamos poder coordinarnos con usted.

Saludos cordiales,

Centro de la asistencia técnica de Cisco (TAC)

Enlaces:

- [1] [Aviso de seguridad oficial \(cisco-sa-sdwan-privesc-4uxFrdzx\)](#)
- [2] [Guía de refuerzo de SD-WAN de Cisco](#)
- [3] [Inicie la actualización de Catalyst SD-WAN](#)
- [4] [Guía de actualización de SD-WAN de Cisco](#)
- [5] [Guía de remediación del TAC](#)

Abrir en Outlook

① Reemplazar todos los [marcadores de posición entre corchetes] antes de enviar.

✉ Abrir Outlook (solo asunto)

↓ Descargar plantilla .eml

Plantilla de TAC 16 para IOC identificado/versión fija no disponible (WAVE 2a — Harden & Await Fix)

caso de uso

Enviados a clientes cuyos registros de SD-WAN mostraban **indicadores de compromiso (IoC)** relacionados con CVE-2026-20245, pero para los que **actualmente no hay ninguna versión de software fija disponible** para su plataforma/versión. Aconseja un endurecimiento inmediato, programa una llamada de revisión e informa al cliente de que debe esperar a que la versión fija solucione los problemas por completo.

Asunto

URGENTE: IoC identificado para CVE-2026-20245 - Versión fija no disponible actualmente - SR [SR#]

Mensaje

Estimado cliente:

Gracias por ponerse en contacto con el centro de asistencia técnica Cisco Technical Assistance Center (TAC) en relación con CVE-2026-20245 en la solicitud de servicio [SR#].

Después de analizar los archivos técnicos de administración proporcionados por los componentes de control de la SD-WAN, nuestro equipo ha **identificado los indicadores de compromiso (IoC)** asociados con CVE-2026-20245.

Dada la gravedad de estas conclusiones, es fundamental que examinemos los detalles técnicos y las medidas provisionales recomendadas lo antes posible. Nos gustaría programar una llamada con su equipo para revisar las conclusiones específicas.

Importante: actualmente no hay ninguna versión de software fija disponible:

En este momento, **no hay ninguna versión de software fija disponible** para su plataforma y versión de software actuales para remediar completamente esta vulnerabilidad. El departamento de ingeniería de Cisco trabaja activamente para ofrecer una versión fija. Una vez que el software fijo esté disponible, el [aviso oficial de seguridad](#)^[1] se actualizará con la información de versión fija.

Acciones inmediatas necesarias:

1. **Programar una llamada de revisión:** Háblenos de si está disponible para realizar una breve llamada en las próximas [p. ej., de 4 a 8 horas] con el fin de revisar las conclusiones del IoC y debatir las medidas de contención provisionales.

2. **Aplique inmediatamente las mejores prácticas de refuerzo:** Revise e implemente las recomendaciones de la [Guía de endurecimiento de SD-WAN de Cisco](#)^[2] para reducir la superficie de ataque mientras espera la versión fija.
3. **Supervisión reforzada:** Supervise estrechamente los componentes de control de la SD-WAN para detectar comportamientos anómalos, cambios de configuración inesperados o intentos de acceso no autorizado.
4. **Supervise el aviso de seguridad:** Consulte periódicamente el [aviso oficial de seguridad](#)^[1] para obtener actualizaciones sobre la disponibilidad de versiones fijas para su plataforma.
5. **Plan de actualización:** Comience a planificar la actualización ahora para estar preparado para ejecutar la actualización rápidamente una vez que se publique la versión corregida.

Pasos siguientes:

Actualizaremos este caso cuando la versión de software fija esté disponible. En ese momento, debe dar prioridad a la actualización de todos los componentes de control de SD-WAN (Manager, Controller, Validator) a la versión fija inmediatamente. Tras la actualización, se tratarán pasos adicionales de remediación (como la reimplementación del controlador y la rotación de certificados) en función de los resultados revisados durante la llamada.

Consulte también la [Guía de remediación del TAC](#)^[3] [para obtener información sobre las opciones de remediación que se aplicarán una vez que la versión fija esté disponible.](#)

Nuestro objetivo principal es ayudarle a proteger su entorno y a mitigar cualquier riesgo potencial. Agradecemos su pronta atención a este asunto y esperamos poder coordinarnos con usted.

Saludos cordiales,

Centro de la asistencia técnica de Cisco (TAC)

Enlaces:

[1] [Aviso de seguridad oficial \(cisco-sa-sdwan-privesc-4uxFrdzx\)](#)

[2] [Guía de refuerzo de SD-WAN de Cisco](#)

[3] [Guía de remediación del TAC](#)

Abrir en Outlook

① Reemplazar todos los *[marcadores de posición entre corchetes]* antes de enviar.

✉ Abrir Outlook (solo asunto)

↓ Descargar plantilla .eml

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).