

Alerta ID:	052
Fecha del reporte:	16/06/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Ataque con privilegios netadmin; Ejecuta comandos arbitrarios como root
Herramienta de detección	N/A
Activo involucrado:	Cisco Catalyst SD-WAN Manager
Tipo de alerta:	Alerta
Nivel de riesgo:	Alto

Objetivo:

Informar a las organizaciones del sector salud en Colombia sobre la identificación de la vulnerabilidad crítica **CVE-2026-20245** en Cisco Catalyst SD-WAN Manager, la cual permite a un atacante autenticado con privilegios elevados ejecutar comandos arbitrarios con privilegios de sistema, comprometiendo la seguridad de la infraestructura de red.

Esta vulnerabilidad podría resultar en el control total del plano de gestión de red (control plane), afectando la disponibilidad, integridad y confidencialidad de los servicios de conectividad que soportan sistemas clínicos y administrativos en el sector salud.

El propósito de esta alerta es que las organizaciones del sector salud validen si están utilizando versiones afectadas de Cisco SD-WAN Manager, ya sea en infraestructura propia, servicios



gestionados o entornos híbridos, revisando inventarios tecnológicos, plataformas de conectividad entre sedes, redes hospitalarias distribuidas, sistemas de telemedicina y demás componentes que dependen de la infraestructura SD-WAN para la operación de servicios críticos.

Descripción:

La vulnerabilidad **CVE-2026-20245** afecta a **Cisco Catalyst SD-WAN Manager**, específicamente en la funcionalidad de gestión y procesamiento de solicitudes dentro del plano de administración (control plane). Esta falla permite que un atacante autenticado con privilegios elevados pueda explotar una validación insuficiente de entradas durante operaciones administrativas, lo que deriva en la ejecución de comandos arbitrarios a nivel de sistema.

El fallo se origina en la forma en que el sistema procesa entradas suministradas a través de la interfaz de gestión, lo que permite que ciertos parámetros no sean adecuadamente validados antes de ser ejecutados por el sistema operativo subyacente. Un atacante con acceso a la consola de administración podría aprovechar esta debilidad para ejecutar instrucciones con privilegios de root.

Esta condición es especialmente crítica en entornos donde Cisco SD-WAN se utiliza para interconectar sedes hospitalarias, sistemas de telemedicina, laboratorios clínicos y plataformas de historia clínica electrónica, ya que comprometer el controlador SD-WAN implica la posibilidad de afectar múltiples sistemas críticos de forma simultánea.

La explotación de esta vulnerabilidad permite comprometer la integridad del sistema de gestión de red, alterar configuraciones de conectividad, afectar la disponibilidad de servicios



interconectados y potencialmente facilitar el acceso a otros sistemas dentro de la infraestructura del sector salud.

La recomendación principal es aplicar los parches de seguridad oficiales de Cisco de manera inmediata, ya que esta vulnerabilidad ha sido clasificada como de alto impacto debido a su potencial de control total sobre la infraestructura de red.

Consecuencias de la explotación

La explotación exitosa de la vulnerabilidad CVE-2026-20245 en Cisco Catalyst SD-WAN Manager puede generar impactos significativos tanto a nivel técnico como operativo en las organizaciones del sector salud. Entre las principales consecuencias se destacan:

1. Acceso no autorizado al plano de gestión de red

Los atacantes que exploten esta vulnerabilidad pueden ejecutar comandos con privilegios elevados dentro del SD-WAN Manager, obteniendo control sobre la infraestructura de red que interconecta sedes hospitalarias, sistemas clínicos y plataformas administrativas.

2. Compromiso total del control de red (Control Plane)

El atacante podría manipular configuraciones del SD-WAN, afectando rutas, políticas de tráfico y segmentación de red, lo que impacta directamente la conectividad entre hospitales, laboratorios y sistemas críticos.

3. Impacto sobre disponibilidad de servicios clínicos

La alteración del tráfico o la desconfiguración del SD-WAN puede generar interrupciones en servicios esenciales como:



- Historia clínica electrónica (HCE)
- Sistemas de laboratorio
- Telemedicina
- Sistemas de facturación y admisión

4. Exposición o manipulación de tráfico sensible

El compromiso del controlador SD-WAN puede permitir la redirección o interceptación del tráfico entre sedes, exponiendo información sensible de pacientes, credenciales y datos administrativos.

5. Movimiento lateral en la infraestructura hospitalaria

Al controlar la red, el atacante puede facilitar el acceso a otros sistemas internos conectados, ampliando el alcance del compromiso dentro del ecosistema tecnológico del sector salud.

6. Riesgos reputacionales

La afectación de servicios críticos o la exposición de información sensible puede impactar la confianza de pacientes, entidades regulatorias y aliados estratégicos del sector salud.

7. Impacto regulatorio y legal

El compromiso de datos sensibles puede generar incumplimientos de normativas como la Ley 1581 de 2012 en Colombia, además de posibles sanciones regulatorias y procesos de auditoría o investigación.

Modo de explotación del ataque

La explotación de la vulnerabilidad **CVE-2026-20245** en **Cisco Catalyst SD-WAN Manager** puede llevarse a cabo mediante las siguientes fases claramente definidas:



Fase 1 – Acceso al panel de administración SD-WAN

El atacante obtiene acceso al entorno de administración de Cisco SD-WAN Manager, ya sea mediante credenciales válidas comprometidas, reutilización de credenciales o acceso interno a la consola de gestión.

Este acceso es un prerequisite clave para la explotación de la vulnerabilidad.

Fase 2 – Manipulación de solicitudes administrativas

El atacante envía solicitudes específicamente diseñadas hacia la interfaz de gestión del sistema, aprovechando una validación insuficiente de entradas en los módulos administrativos.

Esto permite la inyección de comandos o parámetros no sanitizados dentro del sistema.

Fase 3 – Ejecución de comandos a nivel de sistema

La vulnerabilidad permite que las entradas maliciosas sean interpretadas por el sistema operativo subyacente, resultando en la ejecución de comandos con privilegios elevados (root).

Esto otorga control directo sobre el sistema SD-WAN Manager.

Fase 4 – Compromiso del plano de control de red

Una vez con privilegios elevados, el atacante puede:

- Modificar políticas de enrutamiento SD-WAN
- Alterar configuraciones de conectividad entre sedes
- Interrumpir o redirigir tráfico entre hospitales
- Deshabilitar servicios críticos de red



Fase 5 – Impacto en infraestructura hospitalaria conectada

El control del SD-WAN permite afectar múltiples sistemas del sector salud simultáneamente, incluyendo:

- Sistemas de historia clínica electrónica (HCE)
- Plataformas de telemedicina
- Sistemas de laboratorio y diagnóstico
- Servicios administrativos y de facturación

Fase 6 – Movimiento lateral dentro de la red

Con control del plano de red, el atacante puede facilitar el acceso a otros sistemas internos conectados, ampliando el impacto del compromiso dentro de la infraestructura hospitalaria.

Vulnerabilidades asociadas

La vulnerabilidad **CVE-2026-20245** en **Cisco Catalyst SD-WAN Manager** no corresponde a un fallo aislado de ejecución remota independiente, sino a debilidades en la **validación de entradas y control de ejecución dentro del plano de administración del sistema SD-WAN**. Sin embargo, su explotación puede relacionarse con las siguientes condiciones de seguridad mal implementadas:

Validación insuficiente de entradas en interfaces administrativas

- La vulnerabilidad se origina en la falta de validación adecuada de parámetros enviados a través de la consola de administración del SD-WAN Manager, lo que permite que entradas maliciosas sean interpretadas por el sistema operativo subyacente.



- Esto puede derivar en **ejecución de comandos con privilegios elevados (root)**.

Debilidades en el control del plano de gestión (Control Plane)

- El SD-WAN Manager centraliza la administración de la red, por lo que una validación deficiente en sus módulos administrativos permite la manipulación de configuraciones críticas.
- Esto compromete directamente la **integridad de la infraestructura de red del sector salud**.

Exposición de infraestructura crítica interconectada

Una explotación exitosa puede permitir acceso a configuraciones que controlan tráfico entre sedes hospitalarias, sistemas clínicos y plataformas de telemedicina, aumentando el riesgo de:

- Intercepción de tráfico
- Redirección de comunicaciones
- Exposición de servicios internos

Falta de controles de segmentación y privilegios administrativos

- La ausencia o mala implementación de controles como:
- segmentación del plano de gestión
- control de acceso basado en roles (RBAC)
- autenticación multifactor en administración
- incrementa significativamente el impacto de la explotación.

Riesgo de escalamiento dentro de la infraestructura de red

El compromiso del SD-WAN Manager puede facilitar el acceso a otros dispositivos de red, routers, gateways y servicios internos conectados, ampliando el impacto del ataque dentro del ecosistema hospitalario.



Recomendaciones de detección y mitigación



Los equipos de seguridad, infraestructura y administración de TI en las organizaciones del sector salud deben priorizar la actualización inmediata de Cisco Catalyst SD-WAN Manager hacia las versiones corregidas publicadas por el fabricante, con el fin de eliminar la exposición a la vulnerabilidad **CVE-2026-20245**.

Se recomienda verificar todos los entornos donde esté desplegado SD-WAN Manager, incluyendo infraestructura local, entornos en la nube, centros de datos híbridos y plataformas gestionadas por terceros, asegurando que no existan instancias vulnerables que puedan comprometer el plano de control de red.

Medidas prioritarias

1. Actualización inmediata de SD-WAN Manager

Actualizar a la versión corregida recomendada por Cisco, asegurando la eliminación del vector de inyección de comandos en la interfaz de administración.

2. Fortalecimiento del acceso administrativo

- Restringir el acceso al panel de administración SD-WAN
- Aplicar listas blancas de IP para acceso a la consola



- Implementar autenticación multifactor (MFA) para usuarios administrativos

3. Monitoreo de actividad en el plano de gestión

- Alertar accesos inusuales al SD-WAN Manager
- Detectar ejecución de comandos no habituales en la consola administrativa
- Revisar cambios en políticas de enrutamiento o configuración de red

4. Auditoría de configuraciones críticas

- Verificar integridad de políticas SD-WAN
- Revisar cambios en rutas, túneles y segmentación de red
- Validar logs de administración del sistema

5. Segmentación de red y control del control plane

- Aislar el plano de gestión del plano de datos
- Limitar exposición del SD-WAN Manager a redes internas seguras
- Evitar acceso directo desde redes no confiables

6. Revisión de registros y correlación SIEM

- Monitorear intentos de ejecución de comandos desde la consola
- Correlacionar eventos de autenticación con acciones administrativas



- Detectar patrones anómalos de configuración o reinicio de servicios

7. Gestión de privilegios

- Aplicar principio de mínimo privilegio en cuentas netadmin
- Revisar usuarios con acceso administrativo activo
- Deshabilitar cuentas inactivas o no justificadas

8. Validación de despliegues corporativos

- Asegurar consistencia en entornos distribuidos SD-WAN
- Verificar configuraciones en sucursales hospitalarias
- Garantizar que los cambios se propaguen de forma controlada

Recomendaciones de prevención y mitigación

Para prevenir la explotación de la vulnerabilidad CVE-2026-20245 en Cisco Catalyst SD-WAN Manager y fortalecer la seguridad de la infraestructura de red en el sector salud, se recomienda implementar las siguientes medidas de prevención y fortalecimiento:

1. Aplicar actualizaciones de seguridad de inmediato



Instalar la versión corregida de Cisco SD-WAN Manager publicada por el fabricante en todos los entornos afectados, incluyendo infraestructura on-premise, nube híbrida y entornos gestionados por terceros.

2. Fortalecer la seguridad del plano de gestión (Control Plane)

Restringir estrictamente el acceso al panel de administración SD-WAN mediante:

- Listas blancas de IP
- Segmentación de red
- Acceso únicamente desde redes administrativas seguras

3. Implementar autenticación multifactor (MFA)

Habilitar MFA obligatorio para todos los usuarios con privilegios administrativos en el SD-WAN Manager para reducir el riesgo de acceso no autorizado.

4. Aplicar principio de mínimo privilegio

Limitar los roles administrativos (netadmin) solo a personal autorizado, revisando periódicamente cuentas activas y eliminando accesos innecesarios o heredados.

5. Monitoreo y detección de actividad anómala



CSIRTSALUD-AV-20260616-52

TLP: CLEAR

- Implementar monitoreo continuo sobre:
- Cambios en políticas de enrutamiento
- Modificaciones en configuraciones SD-WAN
- Ejecución de comandos administrativos inusuales
- Accesos fuera de horarios o ubicaciones normales

6. Auditoría de configuración de red

- Realizar revisiones periódicas de:
- Políticas de conectividad entre sedes hospitalarias
- Configuración de túneles SD-WAN
- Segmentación de tráfico clínico y administrativo

7. Registro y correlación en SIEM

- Centralizar logs del SD-WAN Manager para:
- Detectar intentos de explotación
- Correlacionar eventos de autenticación con cambios de configuración
- Identificar patrones de comportamiento anómalo en administración de red

8. Segmentación de infraestructura crítica



Separar el plano de gestión del plano de datos, asegurando que el acceso administrativo no esté expuesto a redes no confiables o usuarios finales.

9. Evaluación periódica de vulnerabilidades

Incluir Cisco SD-WAN Manager en programas de gestión de vulnerabilidades, priorizando activos críticos de red hospitalaria.

10. Defensa en profundidad

- Implementar múltiples capas de seguridad:
- Firewalls de red
- Controles de acceso basados en roles (RBAC)
- IDS/IPS
- Monitoreo de tráfico entre sedes
- Políticas estrictas de administración de red.

Recomendaciones de respuesta ante compromiso

En caso de que se confirme un compromiso debido a la explotación de la vulnerabilidad CVE-2026-20245 en Cisco Catalyst SD-WAN Manager, se deben seguir los siguientes pasos para contener el incidente, mitigar el impacto y restaurar la seguridad de la infraestructura de red del sector salud:



1. Aislamiento del sistema comprometido

Desconectar inmediatamente el Cisco SD-WAN Manager afectado del entorno de red o segmentarlo de forma controlada para evitar la propagación del compromiso hacia otros dispositivos de red y sedes hospitalarias.

Si el incidente es crítico, restringir temporalmente el acceso administrativo al sistema.

2. Bloqueo de accesos administrativos

Revocar inmediatamente credenciales sospechosas o comprometidas asociadas a usuarios con rol netadmin o privilegios elevados en el sistema SD-WAN.

Forzar cierre de sesiones activas en la consola de administración.

3. Revisión de configuraciones de red

Auditar cambios recientes en:

- Políticas de enrutamiento SD-WAN
- Configuración de túneles entre sedes
- Segmentación de red hospitalaria
- Reglas de tráfico entre servicios críticos

4. Auditoría de registros y actividades

Realizar análisis exhaustivo de logs del SD-WAN Manager para identificar:

- Ejecución de comandos no autorizados
- Cambios en configuraciones de red
- Accesos inusuales al panel administrativo



- Modificaciones en políticas de conectividad

5. Análisis forense del sistema

Ejecutar análisis forense sobre el sistema comprometido para determinar:

- Alcance del compromiso
- Acciones ejecutadas por el atacante
- Posible persistencia en la configuración del sistema

6. Restauración de configuración segura

Restaurar configuraciones de red desde respaldos confiables y verificados, asegurando que no contengan modificaciones maliciosas.

Aplicar parches oficiales de Cisco antes de reintroducir el sistema en producción.

7. Monitoreo de infraestructura de red hospitalaria

Incrementar la vigilancia sobre:

- Tráfico entre sedes clínicas
- Conectividad de sistemas de historia clínica electrónica (HCE)
- Servicios de telemedicina y laboratorio
- Cambios en rutas o comportamiento del tráfico

8. Notificación del incidente

Informar al equipo de seguridad, CSIRT interno y responsables de infraestructura.

Si existe afectación de datos sensibles o continuidad de servicios de salud, reportar conforme a la Ley 1581 de 2012 en Colombia y normativas aplicables.



9. Verificación de integridad del entorno SD-WAN

Confirmar que:

- No existan configuraciones no autorizadas
- Los dispositivos conectados no hayan sido afectados
- Las políticas de red sean consistentes con el estado previo al incidente

10. Fortalecimiento post-incidente

Implementar mejoras en:

- Segmentación del plano de gestión
- MFA obligatorio para administración SD-WAN
- Monitoreo continuo mediante SIEM
- Principio de mínimo privilegio para cuentas administrativas.

Conclusiones

La vulnerabilidad **CVE-2026-20245** en **Cisco Catalyst SD-WAN Manager** representa un riesgo crítico para la infraestructura de red utilizada en organizaciones del sector salud, debido a su capacidad de permitir la ejecución de comandos con privilegios elevados dentro del plano de administración del sistema.

La explotación de esta vulnerabilidad podría comprometer de forma significativa la **confidencialidad, integridad y disponibilidad** de los servicios de conectividad que soportan sistemas clínicos, administrativos y de telemedicina, afectando la comunicación entre sedes hospitalarias y servicios esenciales de atención.



El impacto de esta vulnerabilidad se extiende tanto a nivel técnico, al comprometer el control centralizado de la red (control plane), como a nivel operativo, al poner en riesgo la continuidad de servicios críticos como historia clínica electrónica, laboratorios y plataformas de atención remota.

La aplicación inmediata de actualizaciones de seguridad proporcionadas por el fabricante, junto con la implementación de controles de acceso estrictos, segmentación de red, monitoreo continuo y fortalecimiento de políticas de administración, es esencial para reducir el riesgo de explotación.

Asimismo, es fundamental que las organizaciones del sector salud realicen revisiones periódicas de su infraestructura SD-WAN, asegurando que los sistemas de conectividad entre sedes se mantengan protegidos, actualizados y correctamente segmentados.

La adopción de estas medidas permitirá fortalecer la seguridad de la infraestructura tecnológica, garantizar la continuidad operativa de los servicios de salud y reducir la exposición a ataques dirigidos contra sistemas de red críticos.

Fuentes:



- **Cisco Security Advisories – Cisco SD-WAN Manager Vulnerability Disclosure**

Documentación oficial de Cisco sobre vulnerabilidades en el componente SD-WAN Manager, incluyendo validación de entradas y ejecución de comandos.

<https://tools.cisco.com/security/center/publicationListing.x>



- **National Vulnerability Database (NVD) – CVE-2026-20245**

Registro oficial de la vulnerabilidad, incluyendo descripción técnica, vector de ataque y métricas CVSS.

<https://nvd.nist.gov/vuln/detail/CVE-2026-20245>

- **CVE.org / MITRE CVE Record**

Referencia oficial del identificador CVE y su descripción técnica asociada.

<https://www.cve.org>

- **Cisco SD-WAN Manager Documentation**

Documentación técnica del producto afectado, arquitectura del plano de control y módulos de administración.

<https://www.cisco.com/c/en/us/products/cloud-systems-management/wan-automation-software/index.html>

- **MITRE ATT&CK Framework for Enterprise**

Referencia para mapeo de técnicas de explotación asociadas a ejecución de comandos, escalamiento de privilegios y compromiso de infraestructura de red.

<https://attack.mitre.org/>

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el **CSIRT Salud** a través de las líneas telefónicas **(+57) 316 893 1490 - 318 155 3570** o mediante el correo electrónico **csirtsalud@minsalud.gov.co**. Nuestro equipo está disponible para brindar el acompañamiento necesario.

