

Alerta ID:	107
Fecha del reporte:	05/06/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Explotación activa de vulnerabilidades en Cisco Catalyst SD-WAN permite compromiso de infraestructura de red empresarial
Herramienta de detección	N/A
Activo involucrado:	Cisco Catalyst SD-WAN Manager (vManage), Cisco Catalyst SD-WAN Controller (vSmart), infraestructura WAN, redes corporativas, centros de datos, entornos híbridos, servicios críticos institucionales
Tipo de alerta:	Alerta
Nivel de riesgo:	Critico

Objetivo:

Informar a las organizaciones del sector salud en Colombia sobre la explotación activa de múltiples vulnerabilidades que afectan componentes Cisco Catalyst SD-WAN, identificadas mediante los CVE-2026-20122, CVE-2026-20128, CVE-2026-20133, CVE-2026-20127 y CVE-2026-20182, las cuales están siendo utilizadas por actores de amenaza para comprometer infraestructura SD-WAN expuesta a Internet.

El propósito de esta alerta es que las entidades evalúen el impacto potencial que estas vulnerabilidades podrían generar sobre:

- infraestructura de comunicaciones corporativas;
- disponibilidad de servicios institucionales;



- redes WAN críticas;
- acceso administrativo a plataformas Cisco;
- segmentación de red;
- continuidad operativa;
- plataformas clínicas conectadas;
- servicios de interoperabilidad;
- infraestructura híbrida y cloud;
- y servicios críticos soportados sobre redes SD-WAN.

Asimismo, se busca generar conciencia sobre los riesgos asociados a la exposición de componentes de administración SD-WAN, credenciales privilegiadas, accesos administrativos remotos y configuraciones insuficientes de endurecimiento sobre infraestructura de comunicaciones institucional.

En el contexto del sector salud, este escenario representa un riesgo significativo debido a la creciente dependencia de:

- redes hospitalarias distribuidas;
- sedes remotas conectadas mediante SD-WAN;
- plataformas clínicas interoperables;
- servicios de telemedicina;
- centros de datos híbridos;
- infraestructura cloud conectada;
- y servicios institucionales críticos soportados sobre redes Cisco.

La explotación exitosa podría facilitar escenarios relacionados con:

- acceso administrativo no autorizado;
- divulgación de información sensible;
- escalamiento de privilegios;
- movimiento lateral;
- modificación de configuraciones de red;



- persistencia dentro de la infraestructura;
- interrupción de servicios críticos;
- y compromiso de la continuidad operativa institucional.

Descripción:

Cisco confirmó la explotación activa de múltiples vulnerabilidades que afectan Cisco Catalyst SD-WAN Manager y Cisco Catalyst SD-WAN Controller, componentes ampliamente utilizados para la administración centralizada de redes empresariales definidas por software (SD-WAN).

Las investigaciones realizadas por Cisco Talos identificaron actividad maliciosa asociada al actor denominado UAT-8616, el cual ha explotado vulnerabilidades de bypass de autenticación para obtener privilegios administrativos sobre dispositivos SD-WAN expuestos.

Los análisis indican que parte de esta actividad podría haberse desarrollado durante varios años antes de su detección.

Entre las vulnerabilidades más relevantes se encuentran:

- CVE-2026-20182 – Authentication Bypass;
- CVE-2026-20127 – Authentication Bypass;
- CVE-2026-20122 – Arbitrary File Overwrite;
- CVE-2026-20128 – Information Disclosure;
- CVE-2026-20133 – Information Disclosure.

Las evaluaciones técnicas indican que un atacante remoto podría:

- obtener acceso administrativo no autorizado;
- acceder a información sensible;
- sobrescribir archivos del sistema;



- obtener credenciales privilegiadas;
- modificar configuraciones SD-WAN;
- establecer persistencia;
- desplegar herramientas maliciosas;
- y comprometer la administración centralizada de la infraestructura WAN.

Uno de los aspectos más relevantes corresponde a que SD-WAN Manager actúa como plataforma centralizada de administración de la infraestructura de comunicaciones. Su compromiso puede otorgar visibilidad y control sobre múltiples dispositivos, sedes, enlaces y segmentos de red distribuidos geográficamente

Consecuencias de la explotación



La explotación exitosa de las vulnerabilidades identificadas en Cisco Catalyst SD-WAN Manager y Cisco Catalyst SD-WAN Controller podría generar impactos significativos sobre la confidencialidad, integridad y disponibilidad de las redes institucionales, especialmente en organizaciones que utilizan infraestructura SD-WAN para interconectar sedes, centros de datos, servicios cloud y aplicaciones críticas.

Uno de los principales riesgos asociados corresponde al compromiso de los componentes centrales de administración de la infraestructura SD-WAN. Debido a que estas plataformas concentran funciones de orquestación, monitoreo, configuración y control de dispositivos distribuidos, un atacante que obtenga acceso privilegiado podría afectar simultáneamente múltiples segmentos de la red institucional.

En escenarios vulnerables, un atacante podría aprovechar las vulnerabilidades para:

- obtener acceso administrativo a la plataforma SD-WAN;
- modificar configuraciones de red;
- crear cuentas privilegiadas;
- alterar políticas de enrutamiento;



- acceder a información sensible de la infraestructura;
- comprometer dispositivos administrados;
- y mantener persistencia dentro del entorno afectado.

Uno de los impactos más críticos corresponde a la posible modificación de configuraciones de red corporativas. Las plataformas Cisco SD-WAN administran elementos fundamentales para la conectividad institucional, incluyendo:

- políticas de tráfico;
- segmentación de red;
- rutas de comunicación;
- enlaces WAN;
- conectividad entre sedes;
- integración con servicios cloud;
- y mecanismos de alta disponibilidad.

La manipulación de estos componentes podría facilitar escenarios relacionados con:

- redirección maliciosa de tráfico;
- interceptación de comunicaciones;
- degradación de servicios;
- interrupción de conectividad;
- pérdida de segmentación de red;
- y afectación de servicios críticos institucionales.

Otro aspecto relevante corresponde a la exposición de información sensible almacenada dentro de la infraestructura de administración SD-WAN. Dependiendo de la configuración afectada, los atacantes podrían obtener acceso a:

- credenciales administrativas;
- tokens de autenticación;



- configuraciones de red;
- información de dispositivos gestionados;
- certificados digitales;
- parámetros de integración;
- y datos relacionados con la arquitectura tecnológica institucional.

La exposición de estos elementos podría facilitar ataques posteriores orientados al compromiso progresivo de la infraestructura tecnológica.

Las vulnerabilidades también podrían facilitar escenarios de movimiento lateral dentro de la red institucional. Una vez comprometida la plataforma central de administración SD-WAN, los atacantes podrían intentar:

- identificar activos críticos;
- enumerar dispositivos conectados;
- acceder a segmentos internos de red;
- comprometer sistemas adicionales;
- obtener acceso a plataformas corporativas;
- y expandir progresivamente el alcance del incidente.

En organizaciones que operan múltiples sedes o entornos distribuidos, el riesgo resulta particularmente relevante debido a la capacidad de administración centralizada que caracteriza a las soluciones SD-WAN.

Otro impacto significativo corresponde a la posible afectación de la integridad de las comunicaciones institucionales. Un atacante con privilegios elevados podría modificar reglas de tráfico o configuraciones de conectividad para:

- alterar rutas de comunicación;
- redireccionar conexiones;
- manipular flujos de datos;
- interferir con servicios críticos;



- degradar el rendimiento de aplicaciones;
- y comprometer la confiabilidad de las comunicaciones corporativas.

En el contexto del sector salud, este escenario representa una amenaza especialmente sensible debido a la creciente dependencia tecnológica sobre:

- sistemas de información hospitalaria;
- plataformas clínicas;
- servicios de telemedicina;
- plataformas de interoperabilidad;
- sistemas administrativos;
- infraestructura cloud híbrida;
- y servicios digitales orientados a la atención de pacientes.

La explotación exitosa podría impactar directamente servicios relacionados con:

- atención clínica;
- consulta de historias clínicas;
- intercambio de información en salud;
- plataformas diagnósticas;
- servicios de autenticación;
- conectividad entre sedes;
- y operaciones institucionales críticas.

Asimismo, los atacantes podrían utilizar el acceso obtenido para desplegar mecanismos de persistencia dentro de la infraestructura comprometida. Dependiendo del nivel de acceso alcanzado, podrían realizar actividades como:

- creación de cuentas administrativas ocultas;
- modificación de configuraciones de seguridad;
- instalación de herramientas maliciosas;
- despliegue de backdoors;



- alteración de registros de auditoría;
- y mantenimiento de acceso prolongado a la infraestructura.

La permanencia no detectada dentro de la plataforma SD-WAN incrementa significativamente el riesgo de compromisos prolongados y ataques dirigidos contra activos estratégicos de la organización.

Las organizaciones también podrían enfrentar impactos relacionados con:

- indisponibilidad operacional;
- interrupción de comunicaciones entre sedes;
- degradación de servicios tecnológicos;
- pérdida de visibilidad sobre la red;
- afectación de procesos institucionales;
- incremento de la superficie de ataque;
- y deterioro de la postura de seguridad organizacional.

Adicionalmente, la explotación de estas vulnerabilidades podría facilitar ataques posteriores relacionados con:

- ransomware sobre infraestructura corporativa;
- exfiltración de información sensible;
- espionaje cibernético;
- sabotaje operacional;
- compromiso de servicios cloud;
- campañas dirigidas contra infraestructura crítica;
- y afectación de los procesos de continuidad del negocio.

El principal riesgo estratégico asociado a este escenario corresponde a que las plataformas SD-WAN constituyen uno de los componentes más sensibles dentro de las arquitecturas de red modernas. Su compromiso puede proporcionar a los atacantes capacidades de administración, visibilidad y control sobre múltiples activos institucionales, incrementando



significativamente el impacto potencial de un incidente de seguridad y la probabilidad de afectaciones operacionales de gran alcance.

Modo de explotación del ataque



Fase 1 – Reconocimiento de infraestructura SD-WAN expuesta

El proceso de explotación inicia cuando un atacante identifica componentes Cisco Catalyst SD-WAN expuestos a Internet o accesibles desde redes comprometidas.

Durante esta etapa, los actores de amenaza realizan actividades de reconocimiento orientadas a identificar:

- instancias Cisco Catalyst SD-WAN Manager (vManage);
- controladores SD-WAN;
- interfaces administrativas expuestas;
- portales de autenticación;
- versiones de software instaladas;
- servicios accesibles remotamente;
- configuraciones de red visibles;
- certificados digitales utilizados por la plataforma;
- y componentes asociados a la infraestructura SD-WAN.

Los atacantes suelen emplear herramientas de descubrimiento, motores de búsqueda especializados, escaneo de servicios y técnicas OSINT para identificar objetivos potencialmente vulnerables.

El objetivo principal consiste en determinar si la organización utiliza versiones afectadas y establecer el nivel de exposición de la infraestructura.



Fase 2 – Enumeración y validación de vulnerabilidades

Una vez identificado el objetivo, el atacante realiza actividades orientadas a validar la presencia de versiones vulnerables.

Durante esta fase podrían analizarse:

- banners de servicios;
- respuestas HTTP y HTTPS;
- versiones de componentes;
- APIs expuestas;
- mecanismos de autenticación;
- interfaces de administración;
- configuraciones accesibles;
- y servicios auxiliares asociados a la plataforma.

La información obtenida permite determinar si el sistema es susceptible a vulnerabilidades conocidas y seleccionar la técnica de explotación más adecuada.

En muchos escenarios, los atacantes automatizan este proceso para identificar múltiples objetivos vulnerables de manera simultánea.

Fase 3 – Explotación inicial de la vulnerabilidad

Posteriormente, el atacante intenta explotar las vulnerabilidades identificadas en los componentes Cisco SD-WAN.

Dependiendo del vector utilizado, la explotación podría facilitar:

- acceso a información sensible;
- manipulación de archivos;



- obtención de credenciales;
- acceso a funcionalidades administrativas;
- evasión de controles de autenticación;
- y acceso inicial a componentes internos de la plataforma.

Las investigaciones realizadas por Cisco indican que algunas de estas vulnerabilidades han sido utilizadas activamente por actores de amenaza para obtener acceso no autorizado a la infraestructura SD-WAN.

Durante esta etapa, el atacante busca obtener el primer punto de apoyo dentro de la plataforma comprometida.

Fase 4 – Obtención de acceso privilegiado

Una vez explotada la vulnerabilidad inicial, el atacante intenta ampliar sus capacidades dentro del entorno SD-WAN.

Las actividades realizadas podrían incluir:

- obtención de privilegios administrativos;
- acceso a interfaces restringidas;
- consulta de configuraciones internas;
- acceso a servicios de gestión;
- manipulación de componentes administrativos;
- creación de sesiones persistentes;
- y exploración de funcionalidades avanzadas de la plataforma.

Debido a que SD-WAN Manager constituye el punto central de administración de la infraestructura, el acceso privilegiado puede proporcionar visibilidad sobre múltiples dispositivos distribuidos dentro de la organización.



Fase 5 – Recolección de información sensible

Posteriormente, los atacantes realizan actividades orientadas a identificar información de valor dentro del entorno comprometido.

La información objetivo puede incluir:

- credenciales administrativas;
- tokens de autenticación;
- certificados digitales;
- configuraciones de red;
- inventarios de dispositivos;
- información de segmentación;
- rutas de comunicación;
- parámetros de integración;
- y datos relacionados con la arquitectura tecnológica institucional.

La recopilación de esta información facilita la planificación de actividades posteriores de movimiento lateral y escalamiento de privilegios.

Fase 6 – Movimiento lateral dentro de la infraestructura

Una vez consolidado el acceso inicial, el atacante podría intentar expandir el compromiso hacia otros componentes de la organización.

Las actividades de movimiento lateral podrían orientarse hacia:

- dispositivos administrados por la plataforma SD-WAN;
- equipos de red corporativos;



- servicios de autenticación;
- infraestructura cloud integrada;
- servidores críticos;
- plataformas de monitoreo;
- sistemas administrativos;
- y aplicaciones institucionales.

El conocimiento adquirido durante las fases anteriores permite identificar relaciones de confianza entre sistemas y aprovecharlas para ampliar progresivamente el alcance del incidente.

Fase 7 – Manipulación de la infraestructura de comunicaciones

Con acceso privilegiado a la plataforma SD-WAN, el atacante podría intentar modificar componentes esenciales de la infraestructura de comunicaciones.

Las acciones potenciales incluyen:

- alteración de políticas de enrutamiento;
- modificación de configuraciones WAN;
- cambios en reglas de segmentación;
- manipulación de túneles seguros;
- alteración de políticas de tráfico;
- redirección de comunicaciones;
- modificación de parámetros de conectividad;
- y cambios sobre mecanismos de alta disponibilidad.

La manipulación de estos elementos puede afectar significativamente la operación institucional y la disponibilidad de servicios críticos.



Fase 8 – Persistencia dentro del entorno comprometido

Posteriormente, los atacantes podrían establecer mecanismos destinados a mantener acceso continuo a la infraestructura.

Entre las actividades observadas habitualmente en este tipo de escenarios se encuentran:

- creación de cuentas administrativas ocultas;
- modificación de configuraciones de seguridad;
- instalación de herramientas de acceso remoto;
- incorporación de credenciales adicionales;
- alteración de controles de monitoreo;
- manipulación de registros;
- y establecimiento de canales persistentes de comunicación.

El objetivo consiste en garantizar acceso prolongado incluso después de que se implementen acciones de remediación parcial.

Fase 9 – Compromiso operacional y afectación institucional

Finalmente, una explotación exitosa podría derivar en impactos significativos sobre la operación institucional.

Dependiendo del nivel de acceso alcanzado, los atacantes podrían:

- interrumpir comunicaciones entre sedes;
- afectar servicios críticos institucionales;
- degradar el desempeño de la red;
- exfiltrar información sensible;
- comprometer sistemas integrados;



- desplegar ransomware;
- sabotear procesos organizacionales;
- alterar servicios de autenticación;
- comprometer infraestructura cloud conectada;
- y afectar la continuidad del negocio.

En el contexto del sector salud, este escenario resulta especialmente relevante debido a la dependencia de redes seguras y altamente disponibles para soportar aplicaciones clínicas, plataformas hospitalarias, servicios de interoperabilidad, telemedicina y demás servicios críticos para la atención y gestión institucional.

Vulnerabilidades asociadas



Riesgos asociados a bypass de autenticación en plataformas SD-WAN

- **Descripción:** Las vulnerabilidades de bypass de autenticación identificadas en Cisco Catalyst SD-WAN permiten que actores maliciosos evadan determinados mecanismos de validación de identidad y obtengan acceso a funcionalidades administrativas sin completar adecuadamente los procesos de autenticación establecidos por la plataforma. Este tipo de debilidad representa una amenaza significativa debido a que afecta directamente los controles de acceso diseñados para proteger la administración centralizada de la infraestructura de red.
- **Impacto:** La explotación exitosa podría facilitar el acceso no autorizado a componentes críticos de gestión SD-WAN, permitiendo a los atacantes consultar información sensible, modificar configuraciones, crear cuentas privilegiadas, comprometer dispositivos administrados y expandir progresivamente el alcance del incidente dentro de la infraestructura institucional.



Exposición de información sensible y credenciales administrativas

- **Descripción:** Algunas de las vulnerabilidades identificadas permiten la divulgación no autorizada de información almacenada dentro de los componentes Cisco SD-WAN. Entre los elementos potencialmente expuestos se encuentran credenciales, configuraciones de red, tokens de autenticación, certificados digitales y otros datos utilizados para la administración de la infraestructura.
 - **Impacto:** La exposición de esta información podría facilitar el acceso privilegiado a sistemas corporativos, la reutilización de credenciales, el compromiso de servicios integrados, el movimiento lateral dentro de la red institucional y el desarrollo de ataques posteriores dirigidos contra activos críticos de la organización.
-

Riesgos asociados a sobrescritura arbitraria de archivos

- **Descripción:** Las vulnerabilidades de sobrescritura arbitraria de archivos permiten que un atacante manipule o reemplace archivos almacenados en componentes vulnerables de Cisco SD-WAN. Este tipo de comportamiento puede afectar archivos de configuración, componentes operativos, registros del sistema o elementos utilizados por los procesos de administración de la plataforma.
 - **Impacto:** La explotación exitosa podría facilitar la alteración de configuraciones de seguridad, la ejecución de código malicioso, el establecimiento de mecanismos de persistencia, la modificación de componentes críticos y el compromiso progresivo de la infraestructura administrada por la plataforma SD-WAN.
-

Riesgos asociados a escalamiento de privilegios

- **Descripción:** Una vez obtenido acceso inicial mediante alguna de las vulnerabilidades identificadas, los atacantes podrían intentar aprovechar relaciones de confianza,



configuraciones inseguras o credenciales expuestas para ampliar los privilegios disponibles dentro del entorno comprometido.

- **Impacto:** El escalamiento de privilegios podría permitir el acceso a funcionalidades administrativas avanzadas, la manipulación de dispositivos de red, la modificación de políticas corporativas, la administración de usuarios privilegiados y el control de componentes estratégicos de la infraestructura institucional.

Exposición sobre infraestructura de comunicaciones corporativas

- **Descripción:** Cisco Catalyst SD-WAN actúa como plataforma centralizada para la administración de comunicaciones entre sedes, centros de datos, entornos cloud y servicios institucionales. El compromiso de estos componentes puede afectar directamente la infraestructura encargada de soportar la conectividad organizacional.
- **Impacto:** Los atacantes podrían modificar rutas de comunicación, alterar políticas de tráfico, redireccionar conexiones, degradar servicios de red y afectar la disponibilidad de las comunicaciones críticas utilizadas por la organización.

Riesgos asociados al movimiento lateral dentro de la red institucional

- **Descripción:** El acceso obtenido sobre plataformas SD-WAN puede proporcionar visibilidad y conectividad hacia múltiples segmentos de la red corporativa. Esta situación incrementa las posibilidades de que un atacante amplíe el compromiso hacia otros sistemas conectados.
- **Impacto:** Una explotación exitosa podría facilitar el reconocimiento interno, el acceso a nuevos activos, la propagación del ataque, el compromiso de servicios adicionales y la expansión progresiva del incidente hacia diferentes áreas tecnológicas de la organización.



Afectación de mecanismos de segmentación y control de tráfico

- **Descripción:** Las soluciones SD-WAN administran políticas de segmentación, priorización y direccionamiento de tráfico entre diferentes componentes de la infraestructura tecnológica. La manipulación de estas configuraciones puede afectar los mecanismos diseñados para separar y proteger los distintos servicios institucionales.
 - **Impacto:** Los atacantes podrían modificar reglas de segmentación, habilitar comunicaciones no autorizadas entre redes, exponer activos internos y aumentar significativamente la superficie de ataque disponible dentro de la organización.
-

Riesgos asociados a persistencia dentro de la infraestructura comprometida

- **Descripción:** Los actores de amenaza que logran comprometer plataformas SD-WAN suelen intentar establecer mecanismos que les permitan mantener acceso continuo al entorno afectado durante períodos prolongados.
 - **Impacto:** La persistencia puede facilitar la realización de actividades de espionaje, exfiltración de información, sabotaje operacional y ejecución de ataques posteriores, dificultando además los procesos de detección, contención y recuperación por parte de los equipos de seguridad.
-

Exposición sobre entornos híbridos y servicios cloud integrados

- **Descripción:** Muchas implementaciones Cisco SD-WAN mantienen integración directa con servicios cloud, centros de datos, plataformas SaaS e infraestructuras híbridas. Estas conexiones amplían el alcance potencial de una explotación exitosa.



- **Impacto:** Los atacantes podrían utilizar el acceso obtenido para comprometer recursos cloud, acceder a servicios externos integrados, manipular configuraciones de conectividad y afectar múltiples entornos tecnológicos desde un único punto de compromiso.
-

Riesgos asociados a la continuidad operativa institucional

- **Descripción:** La infraestructura SD-WAN constituye un componente fundamental para garantizar la disponibilidad de servicios tecnológicos, comunicaciones corporativas y operaciones institucionales distribuidas geográficamente.
 - **Impacto:** La explotación de estas vulnerabilidades podría generar interrupciones operacionales, degradación de servicios críticos, indisponibilidad de aplicaciones institucionales, afectación de procesos misionales y riesgos significativos para la continuidad del negocio.
-

Riesgos para organizaciones del sector salud

- **Descripción:** Las entidades del sector salud dependen cada vez más de redes seguras, interoperables y altamente disponibles para soportar servicios clínicos, administrativos y asistenciales. El compromiso de la infraestructura SD-WAN podría afectar directamente la conectividad necesaria para el funcionamiento de estos servicios.
- **Impacto:** Una explotación exitosa podría impactar la disponibilidad de plataformas clínicas, sistemas de información hospitalaria, servicios de telemedicina, plataformas de interoperabilidad, mecanismos de autenticación institucional y otros servicios críticos relacionados con la atención en salud y la gestión administrativa.



Recomendaciones



Actualizar inmediatamente los componentes afectados

Las organizaciones que utilicen Cisco Catalyst SD-WAN Manager o Cisco Catalyst SD-WAN Controller deben identificar las versiones actualmente desplegadas y verificar si se encuentran afectadas por las vulnerabilidades reportadas.

Cisco ha publicado actualizaciones de seguridad para corregir las vulnerabilidades identificadas y recomienda realizar la actualización a las versiones corregidas lo antes posible. Se recomienda:

- identificar todos los componentes SD-WAN desplegados;
- verificar la versión instalada;
- validar el estado de soporte del fabricante;
- aplicar las actualizaciones recomendadas por Cisco;
- documentar las actividades de remediación realizadas;
- y validar la correcta operación posterior a la actualización.

Restringir la exposición de interfaces administrativas

Las interfaces administrativas de Cisco SD-WAN no deben estar expuestas directamente a Internet salvo que exista una necesidad operativa debidamente justificada y controlada.

Se recomienda:

- limitar el acceso administrativo únicamente a redes autorizadas;
- implementar listas de control de acceso (ACL);
- restringir el acceso mediante VPN corporativa;
- utilizar mecanismos de segmentación de red;
- filtrar conexiones provenientes de ubicaciones no autorizadas;



- y eliminar accesos públicos innecesarios.

Reducir la exposición externa disminuye significativamente la probabilidad de explotación por parte de actores maliciosos.

Fortalecer los mecanismos de autenticación

Las credenciales administrativas constituyen uno de los principales objetivos durante este tipo de ataques.

Las organizaciones deberían:

- implementar autenticación multifactor (MFA);
- aplicar políticas robustas de contraseñas;
- restringir el uso de cuentas compartidas;
- revisar periódicamente privilegios administrativos;
- eliminar cuentas obsoletas;
- y supervisar actividades de autenticación sospechosas.

La autenticación multifactor continúa siendo una de las medidas más efectivas para reducir el riesgo de acceso no autorizado.

Revisar privilegios y accesos administrativos

Es recomendable realizar una revisión integral de los permisos asignados dentro de la plataforma SD-WAN.

La revisión debe incluir:

- usuarios administrativos;



- cuentas de servicio;
- integraciones automatizadas;
- accesos de terceros;
- credenciales utilizadas por herramientas de monitoreo;
- y cuentas asociadas a proveedores.

Los privilegios deben limitarse exclusivamente a las funciones necesarias para cada rol.

Verificar indicadores de compromiso

Debido a la existencia de explotación activa reportada por Cisco, las organizaciones deberían asumir una postura preventiva y validar posibles evidencias de compromiso.

Se recomienda revisar:

- intentos inusuales de autenticación;
 - accesos administrativos no reconocidos;
 - creación de usuarios desconocidos;
 - cambios no autorizados en configuraciones;
 - modificaciones de políticas SD-WAN;
 - eventos relacionados con APIs administrativas;
 - conexiones desde ubicaciones inusuales;
 - y actividades fuera de horario habitual.
-

Monitorear continuamente los registros de auditoría

La supervisión continua puede facilitar la detección temprana de actividades maliciosas. Se recomienda:

- centralizar registros en plataformas SIEM;



- conservar los logs durante periodos adecuados;
- habilitar auditoría detallada de eventos administrativos;
- monitorear cambios de configuración;
- supervisar accesos privilegiados;
- y generar alertas automáticas ante comportamientos anómalos.

Los registros pueden ser fundamentales para procesos posteriores de investigación forense.

Revisar configuraciones de seguridad de la plataforma

Las organizaciones deberían evaluar la postura general de seguridad de sus implementaciones SD-WAN.

Se recomienda validar:

- servicios habilitados;
- puertos expuestos;
- protocolos permitidos;
- configuraciones de acceso remoto;
- mecanismos de administración;
- políticas de cifrado;
- y controles de autenticación implementados.

Los servicios innecesarios deben ser deshabilitados para reducir la superficie de ataque.

Fortalecer la segmentación de red

La segmentación adecuada puede limitar significativamente el impacto de una explotación exitosa.



Se recomienda:

- separar redes administrativas de redes operativas;
- restringir comunicaciones innecesarias;
- implementar controles de microsegmentación cuando sea posible;
- proteger componentes críticos mediante firewalls internos;
- y limitar el acceso entre zonas de seguridad.

La segmentación contribuye a dificultar el movimiento lateral de los atacantes.

Proteger la infraestructura de gestión de red

Los sistemas encargados de administrar la infraestructura tecnológica deben considerarse activos críticos.

Se recomienda:

- aplicar controles reforzados de seguridad;
- restringir el acceso administrativo;
- implementar monitoreo especializado;
- realizar evaluaciones periódicas de vulnerabilidades;
- proteger las estaciones de administración;
- y aplicar principios de mínimo privilegio.

Revisar integraciones con servicios cloud y terceros

Las implementaciones SD-WAN suelen mantener integración con múltiples plataformas externas.

Las organizaciones deberían verificar:



- credenciales utilizadas por integraciones;
 - conexiones hacia entornos cloud;
 - accesos de proveedores;
 - mecanismos de autenticación utilizados;
 - y controles de seguridad implementados en dichas integraciones.
-

Ejecutar actividades de detección proactiva

Las organizaciones con capacidades de monitoreo deberían realizar ejercicios de búsqueda activa de amenazas (Threat Hunting).

Se recomienda buscar:

- accesos administrativos anómalos;
 - creación inesperada de cuentas;
 - modificaciones no autorizadas;
 - actividades asociadas a APIs;
 - cambios sospechosos en políticas de red;
 - conexiones externas inusuales;
 - y patrones de comportamiento compatibles con compromisos previos.
-

Actualizar planes de respuesta a incidentes

Los equipos de seguridad deben verificar que los procedimientos de respuesta contemplen escenarios relacionados con compromisos de infraestructura de red y plataformas SD-WAN.

Se recomienda:

- validar procedimientos de contención;
- actualizar contactos de escalamiento;
- verificar procesos de recuperación;



- revisar respaldos de configuraciones;
 - y realizar simulaciones de incidentes relacionados con infraestructura crítica.
-

Fortalecer la gestión de vulnerabilidades

La explotación activa de estas vulnerabilidades evidencia la importancia de mantener programas formales de gestión de vulnerabilidades.

Las organizaciones deberían:

- realizar escaneos periódicos;
 - mantener inventarios actualizados;
 - priorizar vulnerabilidades explotadas activamente;
 - aplicar parches oportunamente;
 - verificar la efectividad de las remediaciones;
 - y realizar seguimiento continuo de nuevas alertas emitidas por fabricantes.
-

Sensibilizar a administradores y equipos técnicos

Los equipos responsables de redes, infraestructura y ciberseguridad deben conocer los riesgos asociados a la explotación de estas vulnerabilidades.

Se recomienda:

- compartir los boletines de seguridad del fabricante;
- divulgar indicadores de compromiso;
- reforzar procedimientos de monitoreo;
- promover buenas prácticas de administración segura;
- y mantener actualizados los conocimientos técnicos relacionados con plataformas SD-WAN.



Mantener vigilancia permanente sobre nuevas actualizaciones

La situación de amenaza asociada a estas vulnerabilidades continúa evolucionando debido a la explotación activa observada por Cisco y diversos organismos de ciberseguridad.

Por esta razón, se recomienda mantener seguimiento permanente a:

- nuevos boletines de seguridad emitidos por Cisco;
- actualizaciones de indicadores de compromiso;
- nuevas vulnerabilidades relacionadas;
- técnicas de explotación observadas;
- y recomendaciones emitidas por organismos especializados en ciberseguridad.

Conclusiones

Las vulnerabilidades identificadas en Cisco Catalyst SD-WAN Manager y Cisco Catalyst SD-WAN Controller representan una amenaza significativa para las organizaciones que utilizan estas plataformas como componente central de administración y orquestación de sus redes corporativas. La confirmación de explotación activa por parte de Cisco evidencia que estas debilidades han trascendido el ámbito teórico y actualmente están siendo utilizadas por actores maliciosos para comprometer infraestructuras reales.

Uno de los aspectos más relevantes de este escenario corresponde a la posición estratégica que ocupan las soluciones SD-WAN dentro de las arquitecturas tecnológicas modernas. Estos componentes administran la conectividad entre sedes, centros de datos, servicios cloud, plataformas críticas y aplicaciones institucionales, por lo que su compromiso puede proporcionar a un atacante amplias capacidades de control, visibilidad y manipulación sobre la infraestructura de comunicaciones de una organización.



Las investigaciones realizadas por Cisco y diversos organismos especializados en ciberseguridad demuestran que los atacantes continúan enfocando sus esfuerzos sobre plataformas de administración centralizada, aprovechando vulnerabilidades que les permitan obtener acceso privilegiado, evadir controles de seguridad, comprometer configuraciones críticas y establecer mecanismos de persistencia dentro de los entornos afectados.

El riesgo asociado a estas vulnerabilidades no se limita únicamente a la afectación de dispositivos o componentes específicos. Una explotación exitosa podría facilitar escenarios de movimiento lateral, exposición de información sensible, escalamiento de privilegios, manipulación de configuraciones de red, interrupción de servicios críticos y compromiso progresivo de múltiples activos institucionales interconectados.

En el contexto del sector salud, este escenario adquiere una relevancia aún mayor debido a la creciente dependencia de infraestructuras digitales distribuidas para soportar servicios clínicos, administrativos y asistenciales. Las redes SD-WAN se han convertido en un elemento fundamental para garantizar la conectividad entre hospitales, centros médicos, sedes administrativas, plataformas de interoperabilidad, servicios de telemedicina y entornos cloud, por lo que cualquier afectación sobre estos componentes puede generar impactos directos sobre la operación institucional y la prestación de servicios.

La explotación de estas vulnerabilidades también pone de manifiesto la importancia de adoptar enfoques integrales de ciberseguridad que contemplen no solo la aplicación oportuna de actualizaciones de seguridad, sino también el fortalecimiento de controles de acceso, la implementación de mecanismos robustos de autenticación, la segmentación adecuada de redes, el monitoreo continuo de eventos de seguridad y la gestión permanente de vulnerabilidades.

Asimismo, este incidente resalta la necesidad de mantener inventarios actualizados de activos tecnológicos, realizar evaluaciones periódicas de exposición, fortalecer los procesos de detección temprana y garantizar que las organizaciones cuenten con capacidades adecuadas de respuesta y recuperación frente a incidentes que involucren infraestructura crítica de comunicaciones.



Las entidades que utilicen soluciones Cisco Catalyst SD-WAN deben considerar esta situación como una oportunidad para revisar integralmente su postura de seguridad, validar el estado de actualización de sus plataformas, identificar posibles indicadores de compromiso y reforzar las medidas de protección asociadas a la administración de infraestructura de red.

Finalmente, el CSIRT Salud recomienda a todas las organizaciones del sector realizar una evaluación inmediata de los componentes potencialmente afectados, aplicar las actualizaciones de seguridad emitidas por el fabricante, fortalecer los mecanismos de monitoreo y mantener vigilancia permanente sobre nuevas alertas, indicadores de compromiso y actividades de explotación relacionadas con estas vulnerabilidades. La adopción oportuna de medidas preventivas y correctivas permitirá reducir significativamente la probabilidad de compromiso y fortalecer la resiliencia operativa de las infraestructuras tecnológicas que soportan los servicios esenciales del sector salud.

Fuentes:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa-EHchtZk>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-authbp-qwCX8D4v>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-mltvnps2-JxpWm7R>
- <https://securityonline.info/under-attack-cisco-urges-immediate-action-as-hackers-actively-exploit-sd-wan-manager-flaws/>
- <https://www.bleepingcomputer.com/news/security/cisco-flags-more-sd-wan-flaws-as-actively-exploited-in-attacks/>
- <https://securityonline.info/cisco-sd-wan-vulnerability-exploited/>

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.

