Boletín informativo
Vulnerabilidad en Cisco Catalyst SD-WAN

CSIRTSALUD-AV-20260302-32 **TLP: CLEAR**

Incidente ID:	032
Fecha del reporte:	02/03/2026
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Vulnerabilidad en Cisco Catalyst SD-WAN
Herramienta de detección	N/A
Activo involucrado:	CISCO
Tipo de incidente:	Boletín informativo
Nivel de riesgo:	Medio

Objetivo:

Informar a las entidades del Ecosistema sobre la vulnerabilidad crítica de día cero (CVE-2026-20127) que afecta a los productos Cisco Catalyst SD-WAN (Controller/vSmart y Manager/vManage). Este documento detalla la naturaleza de la amenaza, su método de explotación (activo desde 2023 por el grupo UAT-8616), y proporciona las medidas inmediatas para su detección y remediación.

Descripción:

Actores de amenazas altamente sofisticados (rastreados por Cisco Talos como **UAT-8616**) han estado explotando la vulnerabilidad **CVE-2026-20127** en entornos de Cisco SD-WAN expuestos a Internet. El ataque permite a los ciberdelincuentes evadir la autenticación del sistema e insertar un dispositivo falso o *rogue peer* en el plano de control (management/control plane) de la red SD-WAN de la organización afectada.

Una vez que el actor de amenazas obtiene este acceso inicial con altos privilegios, utiliza mecanismos integrados del sistema para realizar un *downgrade* (degradación) del software, explotando una segunda vulnerabilidad más antigua para convertirse en usuario *raíz (root)*. Finalmente, restauran el sistema a su versión original para borrar sus huellas, logrando una persistencia profunda e indetectable.

Consecuencias de la Explotación: El éxito de este ataque representa una brecha crítica para cualquier organización, derivando en las siguientes consecuencias:

- **Compromiso Total de la Red:** Al obtener acceso *root* en los controladores (vSmart) y gestores (vManage), los atacantes logran el control absoluto sobre cómo se enruta y gestiona el tráfico entre sucursales, centros de datos y entornos en la nube.

- **Manipulación e Intercepción de Tráfico:** Los ciberdelincuentes pueden alterar las configuraciones de red mediante NETCONF para interceptar datos confidenciales, redirigir el tráfico hacia servidores maliciosos o denegar el servicio (DoS) a partes críticas de la infraestructura.

- **Movimiento Lateral Sin Restricciones:** El acceso al plano de gestión permite a los atacantes moverse lateralmente hacia otros dispositivos de la red interna que confían en el controlador SD-WAN, extendiendo el alcance del ciberataque mucho más allá del perímetro inicial.

- **Persistencia Profunda (Backdoors):** La modificación de scripts de inicio y la inserción de llaves SSH personalizadas garantizan que los atacantes mantengan su acceso incluso si el dispositivo se reinicia o, en algunos casos, si se aplican parches superficiales sin realizar una reinstalación limpia del sistema.

- **Pérdida de Confidencialidad e Integridad:** La capacidad del atacante para purgar registros (*logs*) y borrar historiales deja a los equipos de seguridad "a ciegas", dificultando enormemente la evaluación del alcance real del robo de datos o la manipulación de la infraestructura.

Productos afectados:

La vulnerabilidad **CVE-2026-20127** afecta a los siguientes productos cuando tienen puertos expuestos a Internet (independientemente de si la implementación es On-Premise o alojada en la nube por Cisco):

- **Cisco Catalyst SD-WAN Controller** (anteriormente conocido como *vSmart*).
- **Cisco Catalyst SD-WAN Manager** (anteriormente conocido como *vManage*).

Versiones Vulnerables y Versiones Corregidas (Parcheadas):

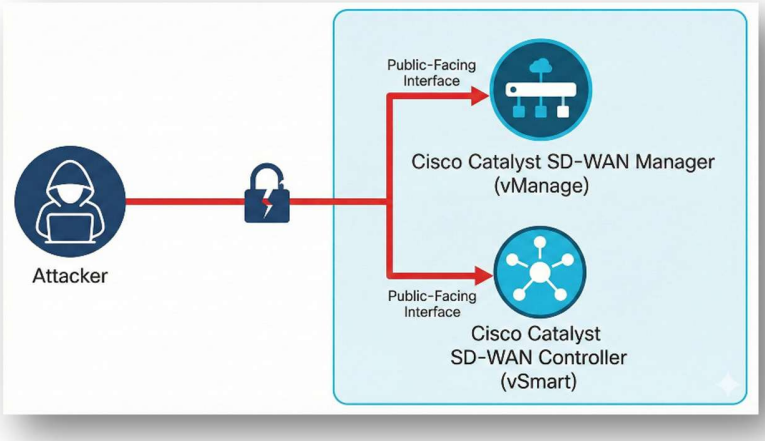
Cisco ha instado a los administradores a actualizar inmediatamente a una versión de software corregida. A continuación, se detallan las ramas de versiones afectadas y a qué versión exacta se debe actualizar para mitigar el fallo:

Rama de Versión (Software Release)	Estado de Vulnerabilidad	Versión Corregida (Recomendada)
Anteriores a 20.9.x	**Vulnerables**	Se debe migrar a una versión soportada y corregida.
Versiones 20.3.1 a 20.14.3	**Vulnerables**	Actualizar a **20.14.4** (o superior según la rama).
Rama 20.9.x	**Vulnerable**	Actualizar a **20.9.8.2**
Rama 20.11.x / 20.12.x	**Vulnerables**	Actualizar a **20.12.6.1**
Rama 20.15.x (incluye 20.15.1)	**Vulnerable**	Actualizar a **20.15.2** (o 20.15.4.2 según disponibilidad)
Rama 20.16.x / 20.18.x	**Vulnerables**	Actualizar a **20.18.2.1**

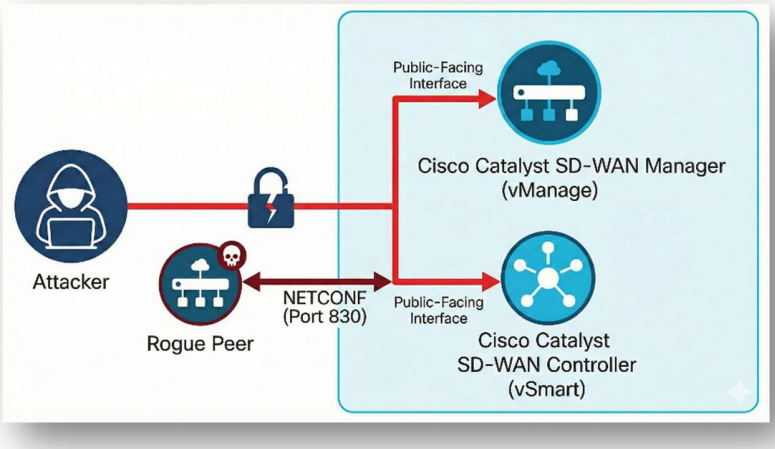
Modo de explotación y cadena de infección

La explotación exitosa llevada a cabo por el actor de amenazas UAT-8616 no se basa en un solo *exploit*, sino en una cadena de ataque (*exploit chain*) sofisticada que abusa de la arquitectura de confianza del tejido SD-WAN de Cisco. El ciclo de vida del ataque se divide en las siguientes fases técnicas:

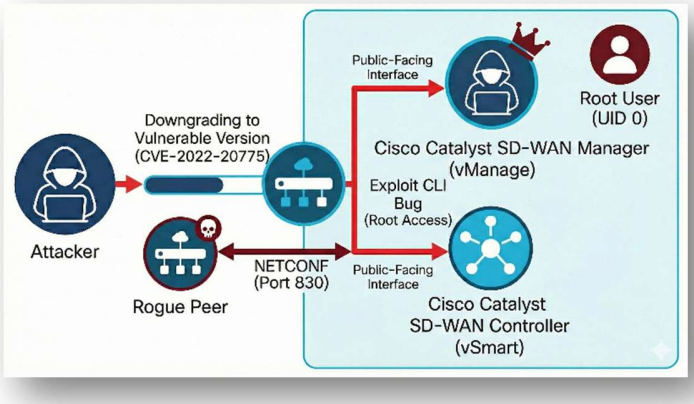
1. Evasión de Autenticación y Acceso Inicial (CVE-2026-20127): El ataque comienza apuntando a instancias de Cisco Catalyst SD-WAN Controller (vSmart) o Manager (vManage) que tengan puertos de gestión expuestos a Internet. La vulnerabilidad (CVSS 10.0) reside en un fallo lógico dentro del mecanismo de autenticación de pares (*peering authentication*). El atacante envía solicitudes de red especialmente manipuladas que explotan la validación deficiente en este proceso. Al hacerlo, logra evadir el intercambio de certificados o credenciales legítimas, instanciando una sesión autenticada con un nivel de privilegio interno elevado (típicamente a nivel de la cuenta vmanage-admin), aunque sin acceso root a nivel de sistema operativo en esta etapa.



2. Inserción de "Rogue Peer" y Abuso de NETCONF: Aprovechando la sesión de altos privilegios recién adquirida, el atacante inyecta un componente SD-WAN controlado por ellos mismos (*rogue peer*) uniéndolo al plano de gestión o plano de control de la red. Este nodo temporal y falso es aceptado como un elemento de confianza en la topología. Desde este *rogue peer*, el atacante inicia conexiones laterales hacia otros *appliances* de la red utilizando **SSH** y el protocolo **NETCONF (TCP/puerto 830)**. Esto les permite leer y modificar la estructura XML de configuración del tejido SD-WAN.



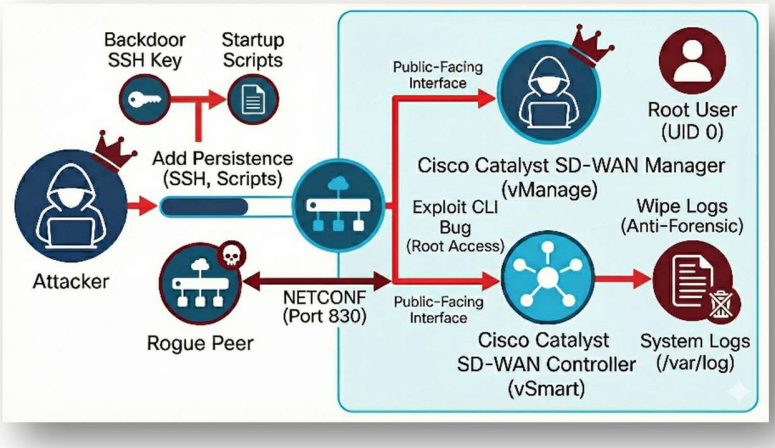
3. Degradación de Firmware (*Downgrade*): Dado que el acceso obtenido en la Fase 1 no otorga control absoluto a nivel de kernel/sistema operativo, el atacante utiliza las propias herramientas de administración integradas del sistema SD-WAN (vía CLI o API) para orquestar un *downgrade* de la imagen del software. Obligan al sistema a arrancar en una versión de firmware anterior que contiene vulnerabilidades conocidas no parcheadas, preparando el terreno para el siguiente paso.



4. Escalamiento de Privilegios a Root (CVE-2022-20775): Una vez que el sistema se reinicia en la versión degradada y vulnerable, el atacante explota localmente la **CVE-2022-20775** (CVSS 7.8). Esta vulnerabilidad específica es un fallo en la validación de entrada dentro de la Interfaz de Línea de Comandos (CLI) de Cisco SD-WAN. A través de técnicas de inyección de comandos o escape de *shell restringida*, el atacante logra ejecutar código arbitrario en el sistema operativo Linux subyacente con privilegios máximos (root).

5. Establecimiento de Persistencia Avanzada: Como superusuario (root), el atacante consolida su acceso mediante las siguientes acciones:

- Creación de cuentas de usuario locales furtivas, con nombres que imitan convenciones de nomenclatura del sistema para pasar desapercibidas.
- Modificación del archivo sshd_config para permitir el acceso (ej. PermitRootLogin) y adición de sus propias llaves públicas SSH en el archivo ~/.ssh/authorized_keys del usuario root y de la cuenta vmanage-admin.
- Alteración de los *scripts* de inicio del sistema SD-WAN (*startup scripts*) para garantizar que las configuraciones maliciosas (backdoors) sobrevivan a reinicios del equipo.



6. Restauración del Sistema y Anti-Forense (Evasión de Defensas): Para ocultar la intrusión a los administradores de red y sistemas de monitoreo de integridad, el atacante utiliza nuevamente el mecanismo de actualización para restaurar el firmware a su versión original (la versión en la que se encontraba antes de la Fase 3). Finalmente, ejecutan tácticas de limpieza extremas: purgan los archivos dentro de /var/log (eliminando o truncando el auth.log), borran el historial de comandos de la terminal (.bash_history) y limpian las tablas de historial de conexiones de red, rompiendo efectivamente la cadena forense local.

Relación con las Tácticas según MITRE ATT&CK

Las acciones observadas por el actor de amenazas se mapean a las siguientes tácticas y técnicas del framework MITRE ATT&CK:

- **Acceso Inicial (Initial Access):** *T1190 - Exploit Public-Facing Application*. Se comprometen dispositivos expuestos a Internet usando la CVE-2026-20127.

- **Ejecución (Execution):** *T1059 - Command and Scripting Interpreter*. El atacante abusa del servicio NETCONF y de conexiones SSH para ejecutar comandos en el sistema.

- **Escalamiento de Privilegios (Privilege Escalation):** *T1068 - Exploitation for Privilege Escalation*. El atacante aprovecha el *downgrade* para explotar la CVE-2022-20775 y obtener nivel *root*.

- **Persistencia (Persistence):** *T1098 - Account Manipulation* y *T1136 - Create Account*. El atacante crea usuarios falsos y añade llaves SSH autorizadas para mantener acceso remoto.

- **Evasión de Defensas (Defense Evasion):** *T1070 - Indicator Removal*. Borrado deliberado de registros de auditoría e historiales de comandos. Además, usan un *Downgrade/Upgrade* para ocultar el exploit secundario.

- **Movimiento Lateral (Lateral Movement):** *T1021 - Remote Services*. Uso de SSH y NETCONF entre las diferentes aplicaciones de gestión y dispositivos interconectados en la topología SD-WAN.

Indicadores de compromiso:

Para identificar si la infraestructura ha sido comprometida, se deben buscar los siguientes indicadores:

- Entradas en el archivo /var/log/auth.log que muestren "Accepted publickey for vmanage-admin" desde direcciones IP desconocidas o no autorizadas.
- Creación o eliminación de cuentas de usuarios locales (a menudo con nombres que imitan a los usuarios legítimos) o inicios de sesión *root* inesperados.

- Presencia de nuevas llaves públicas SSH añadidas en las cuentas vmanage-admin o root.

- Cambios en el sistema que habiliten PermitRootLogin.

- Archivos de registro inusualmente pequeños o faltantes en el directorio /var/log, lo que indica un intento de borrado de evidencia.

- Reinicios inesperados o eventos de degradación (*downgrade*) de la versión del software.

- Revisar la existencia de actividad anómala en los logs /var/volatile/log/vdebug, /var/log/tmplog/vdebug y /var/volatile/log/sw_script_synccdb.log.

- Archivos de historial faltantes o borrados, como `bash_history` o `cli-history`

Recomendaciones de mitigación:

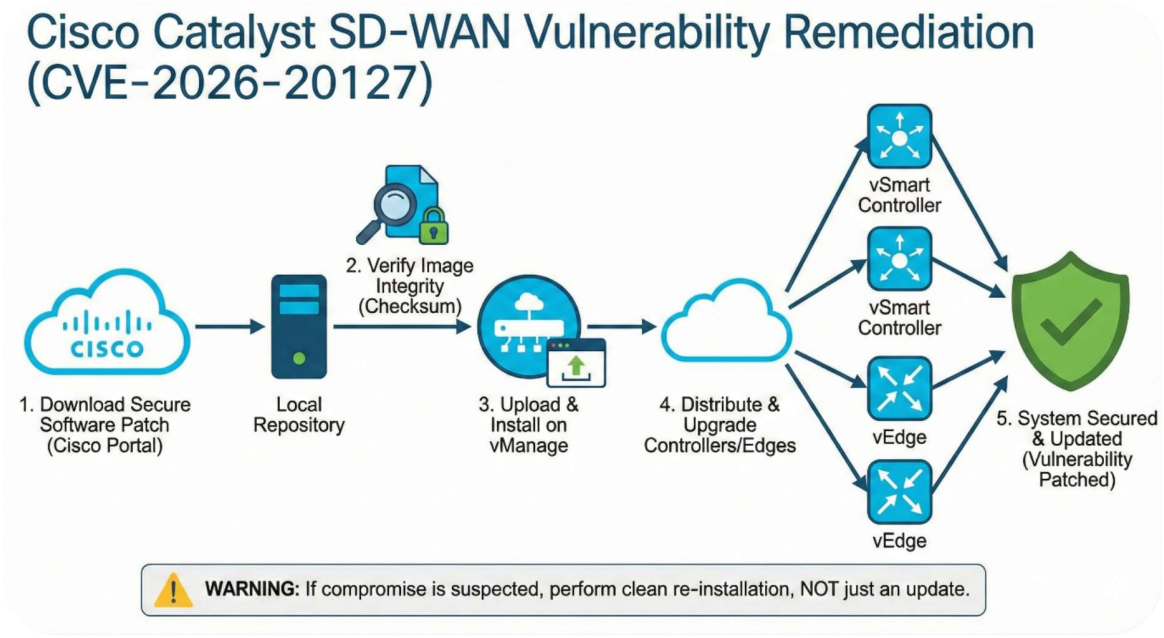
La única forma de mitigar completamente la vulnerabilidad **CVE-2026-20127** es actualizando los dispositivos afectados a las versiones de software corregidas por Cisco. A continuación, se detalla el procedimiento estándar para obtener e instalar el parche.

Si durante la fase de detección (revisión de IoCs) se confirma que los dispositivos ya han sido comprometido, **NO proceder con una simple actualización**. Las agencias de ciberseguridad (CISA/NCSC) dictaminan que el atacante (UAT-8616) mantiene persistencia a nivel *root*. En caso de compromiso confirmado, se debe aislar el equipo, revocar todas las credenciales/certificados y realizar una **instalación limpia (desde cero)** del sistema operativo utilizando una imagen segura.

Para descargar el software oficial, el administrador debe contar con una cuenta de Cisco (CCO) con un contrato de soporte técnico activo (entitlement) vinculado a los equipos SD-WAN.

1. Ingresar a la página oficial de descargas de Cisco: software.cisco.com y navegue a la sección **Software Download**.

2. En la barra de búsqueda, ingresar **"Catalyst SD-WAN Manager"** (para vManage) o **"Catalyst SD-WAN Controller"** (para vSmart).
3. En el panel izquierdo, seleccionar la rama de software que utiliza su infraestructura (por ejemplo, la rama *20.15.x* o *20.14.x*).
4. Ubicar la versión con la corrección de seguridad recomendada (ej. 20.14.4 o 20.15.2). Descargar el archivo de imagen del software (generalmente en formato .tar.gz o un archivo de actualización específico del sistema).



El proceso de actualización en la arquitectura Cisco SD-WAN está centralizado. Se debe seguir un orden estricto de actualización: **Primero se actualiza el Manager (vManage), luego los orquestadores (vBond) y finalmente los Controladores (vSmart)**.

1. **Carga del Software al Repositorio:**
   - Iniciar sesión en la interfaz web de Cisco Catalyst SD-WAN Manager (vManage).
   - Navegar a **Maintenance > Software Repository** (Mantenimiento > Repositorio de Software).
   - Haga clic en **Add New Software** (Agregar nuevo software) y suba el archivo .tar.gz que descargó en la Fase 1.
2. **Distribución e Instalación de la Imagen:**
   - Navegar hasta **Maintenance > Software Upgrade** (Mantenimiento > Actualización de Software).
   - Seleccionar los dispositivos que desea actualizar (comenzando por el propio vManage).
   - Haga clic en el botón **Upgrade** (Actualizar).
   - En el menú desplegable, seleccionar la nueva versión de software que acaba de subir al repositorio y confirme la acción. El sistema distribuirá la imagen y la instalará en la partición inactiva del disco.
3. **Activación de la Nueva Versión:**
   - Una vez que el estado de la instalación muestre "Success" (Éxito), el dispositivo aún estará ejecutando la versión antigua.
   - En la misma pantalla de **Software Upgrade**, seleccione nuevamente los dispositivos.
   - Haga clic en **Activate** (Activar).
   - El dispositivo se reiniciará automáticamente. Durante este proceso, cambiará a la partición que contiene la nueva versión parcheada.
4. **Verificación Post-Actualización:**
   - Una vez que el sistema vuelva a estar en línea, navegar hasta **Monitor > Network** (o *Devices*) para confirmar que la versión de software actual refleja el parche de seguridad (ej. 20.15.2) y que el panel de control muestra todos los dispositivos sincronizados y sin errores de certificados.

Fuentes:

- https://thehackernews.com/2026/02/cisco-sd-wan-zero-day-cve-2026-20127.html
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- https://csirt.telconet.net/comunicacion/boletines-servicios/vulnerabilidad-critica-en-cisco-catalyst-sd-wan-permite-acceso-raiz/
- https://cybersecuritynews.com/cisco-sd-wan-0-day-vulnerability/
- https://blog.elhacker.net/2026/03/vulnerabilidad-critica-de-dia-cero-en.html
- https://www.bleepingcomputer.com/news/security/critical-cisco-sd-wan-bug-exploited-in-zero-day-attacks-since-2023/
- https://www.bleepingcomputer.com/news/security/critical-cisco-sd-wan-bug-exploited-in-zero-day-attacks-since-2023/
- https://www.cve.org/CVERecord?id=CVE-2026-20127

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 8931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.