Boletín de alerta

Boletín Nro.: 50
Fecha de publicación: 14/05/2026
Tema: Alerta 2026-50 Zero□Day en Cisco Catalyst SD□WAN permite control total del fabric vía auth bypass
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

La vulnerabilidad afecta a:

- Cisco Catalyst SD□WAN Controller (antes vSmart), versiones específicas de la rama 20.x usadas como plano de control.
- Cisco Catalyst SD□WAN Manager (antes vManage), versiones 20.x afectadas según tabla de Cisco.

Descripción

Se ha publicado recientemente una vulnerabilidad identificada como **CVE□2026□20127** es una vulnerabilidad de tipo **bypass de autenticación** en el mecanismo de peering de Cisco Catalyst SD□WAN Controller y Manager que permite a un atacante remoto, no autenticado, obtener **privilegios administrativos** en el plano de control SD□WAN. La vulnerabilidad se debe a una validación incorrecta en la autenticación de peers, lo que permite el registro de un peer malicioso o el acceso a una cuenta interna de alto privilegio sin credenciales válidas.

La severidad es **CVSS 10.0 (máxima)** y hay evidencia de explotación activa desde al menos 2023 por parte de un grupo rastreado como **UAT□8616**, lo que llevó a Cisco y a varios CERT a emitir alertas de emergencia. Un exploit exitoso permite al atacante conectarse como usuario interno privilegiado, acceder a **NETCONF** y modificar la configuración de toda la **SD□WAN fabric**, con impacto directo en confidencialidad, integridad y disponibilidad del tráfico corporativo.

Clase de vulnerabilidad

- **Tipo:** Improper Authentication / Authentication Bypass (CWE□287).
- **Componentes afectados:**
  - Peering authentication de Catalyst SD□WAN Controller (control plane).
  - Mecanismo de autenticación de la API y/o funcionalidades asociadas en Catalyst SD□WAN Manager, con CVEs relacionados (CVE□2026□20128, CVE□2026□20129) ampliando la superficie.

La raíz del problema está en que el componente que valida peers y/o peticiones API no verifica correctamente la autenticidad de ciertos mensajes, permitiendo que un atacante remoto se presente como un peer legítimo o abuse rutas lógicas de autenticación.

Vector y alcance

De forma simplificada, el atacante:

- Puede alcanzar el **Control/Management plane** de SD‑WAN Controller/Manager desde Internet o desde una red no confiable (según cómo esté expuesto el entorno).
- Envía **peticiones especialmente construidas** a los servicios de peering o API.
- Debido al fallo de autenticación, el sistema los acepta y asigna un contexto de **usuario interno de alto privilegio** (en Manager, rol netadmin; en Controller, cuenta interna non‑root pero altamente privilegiada).
- Con ese contexto, el atacante puede:
  - Establecer sesiones NETCONF contra el Controller.
  - Modificar políticas, rutas, listas de control de acceso, parámetros de túneles, etc.
  - Instalar rutas maliciosas, redirigir tráfico, desbordar o apagar sitios remotos, o incluso preparar movimientos laterales hacia on‑prem y nubes.

Cisco y distintos vendors indican que se han observado **peers maliciosos** inyectados en el plano de control y escaladas a root posteriores al primer acceso, dentro de campañas atribuidas a UAT‑8616.

Mitigación

Mientras se evalúa y ejecuta el plan de actualización, se recomiendan medidas de mitigación inmediatas:

1. **Reducción de superficie de exposición**
2. Verificar qué instancias de **Catalyst SD‑WAN Controller y Manager** son accesibles desde Internet o redes de menor confianza.
3. Limitar el acceso a estas consolas y puntos de peering a través de:
    1. ACLs en firewalls,
    1. VPN dedicada para administración,
    1. Restricción por IP de origen (rangos de NOC, jump hosts, etc.).
4. **Endurecimiento de accesos**
5. Aplicar **MFA** y controles de bastionado para cualquier acceso administrativo a SD‑WAN Manager (aunque no elimina el bypass de peering, reduce otros vectores).
6. Revisar y minimizar las cuentas con rol netadmin y otros roles de alto privilegio; revocar accesos no necesarios.
7. **Monitorización y hunting**
8. Revisar logs de SD‑WAN Manager/Controller en busca de:

- Nuevos peers registrados o cambios inusuales en la topología de la fabric.
- Conexiones NETCONF no habituales.
- Logins desde IPs anómalas o que no corresponden a tu NOC/SOC.

- Correlacionar con tus fuentes de threat intel por IoC específicos de campañas UAT□8616.

Solución:

Cisco ha publicado versiones corregidas tanto para Controller como para Manager:

- **Catalyst SD□WAN Controller (vSmart)**
  - Actualizar a las versiones **fijas indicadas en el advisory cisco-sa-sdwan-rpa-EHchtZk**, típicamente ramas 20.18.x o posteriores según plataforma.
- **Catalyst SD□WAN Manager (vManage)**
  - Actualizar a **20.18 o superior**, versiones marcadas como no afectadas por CVE□2026□ 20127/20128/20129.

Antes de aplicar los parches, se recomienda validar la nueva versión de Cisco Catalyst SD□WAN en un entorno de pre□producción, comprobando compatibilidad con plantillas, dispositivos edge y políticas, y asegurando backups y snapshots actualizados. Tras planificar una ventana de mantenimiento, se debe actualizar primero SD□WAN Manager y luego los Controllers, siguiendo el orden indicado por Cisco, monitorizando el estado de la fabric y la convergencia de rutas después del cambio. Dado que la vulnerabilidad ya se explota en el mundo real, es prudente asumir que los sistemas vulnerables expuestos antes del parche pueden haber sido comprometidos, por lo que se debe revisar la configuración en busca de cambios no autorizados, rotar todas las credenciales asociadas a SD□WAN (cuentas administrativas, claves, tokens de API) y buscar posibles artefactos o túneles sospechosos dentro de la fabric.

Cisco indica explícitamente que **no hay workarounds completos** y que la acción principal es actualizar.

Información adicional:

- Cisco – **Cisco Catalyst SD?WAN Controller Authentication Bypass (cisco-sa-sdwan-rpa-EHchtZk)**
- NVD – **CVE?2026?20127**
- Tenable – **CVE?2026?20127: Cisco Catalyst SD?WAN Controller/Manager Zero?Day Auth Bypass**
- Cisco Talos – **Ongoing exploitation of Cisco Catalyst SD?WAN**
- The Hacker News – Artículo sobre “Cisco Catalyst SD□WAN Controller Auth Bypass”
- SentinelOne – **CVE?2026?20129 / CVE?2026?20128 – Auth Bypass in Cisco SD?WAN Manager**