Boletín de alerta

Boletín Nro.:
Fecha de publicación: 02/03/2026
Tema: Alerta 2026-20 Vulnerabilidad critica en Cisco SD-WAN
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

La vulnerabilidad afecta a los siguientes componentes de Cisco Catalyst SD-WAN:

- **SD-WAN Controller (vSmart)**

Versiones afectadas: 20.3.1 – 20.14.3, 20.15.1

- **SD-WAN Manager (vManage)**

Versiones afectadas: 20.3.1 – 20.14.3, 20.15.1

Aplica para implementaciones locales y en la nube, incluyendo entornos estándar, gestionados y FedRAMP.

Descripción

Se ha reportado una vulnerabilidad crítica denominada como **CVE-2026-20127** (CVSS 10.0), la cual está siendo explotada activamente desde 2023. La falla se origina en un error en el mecanismo de autenticación de peering del sistema SD-WAN.

La vulnerabilidad permite que un atacante remoto, sin necesidad de credenciales ni interacción del usuario, envíe solicitudes manipuladas para omitir la autenticación. Como resultado, el atacante puede acceder con altos privilegios y modificar la configuración completa de la red SD-WAN, incluyendo:

- Alterar rutas de red
- Agregar dispositivos o peers maliciosos
- Manipular configuraciones críticas

Solución:

Actualizar inmediatamente a las versiones corregidas:

- **SD-WAN Controller (vSmart)**

Versiones corregidas: 20.14.4, 20.15.2

- **SD-WAN Manager (vManage)**

Versiones corregidas: 20.14.4, 20.15.2

Cisco Catalyst SD-WAN Release	Primera versión corregida
Antes de 20.9[1]	Migrar a una versión fija.
20.9	20.9.8.2
20.11[1]	20.12.6.1
20.12	20.12.5.3 20.12.6.1
20.13[1]	20.15.4.2
20.14[1]	20.15.4.2
20.15	20.15.4.2
20.16[1]	20.18.2.1
20.18	20.18.2.1

Para obtener mas información de como actualizar el SD-WAN, puede seguir el siguiente enlace:

https://www.cisco.com/c/dam/en/us/td/docs/Website/enterprise/catalyst-sdwan-upgrade-matrix/index.html

Información adicional:

- **https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa-EHchtZk**
- **Blog elhacker.NET: Vulnerabilidad crítica de día cero en Cisco SD-WAN explotada desde 2023 para obtener acceso root**
- **https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2026-019/**
-