Una vulnerabilidad de omisión de autenticación en el controlador Cisco Catalyst SD-WAN está siendo explotada para obtener acceso de administrador

Cisco publicó actualizaciones para corregir una vulnerabilidad crítica de omisión de autenticación en Catalyst SD-WAN Controller, la cual, según la compañía, ya ha sido aprovechada en ataques limitados.

La falla, identificada como CVE-2026-20182, posee una puntuación CVSS de 10.0.

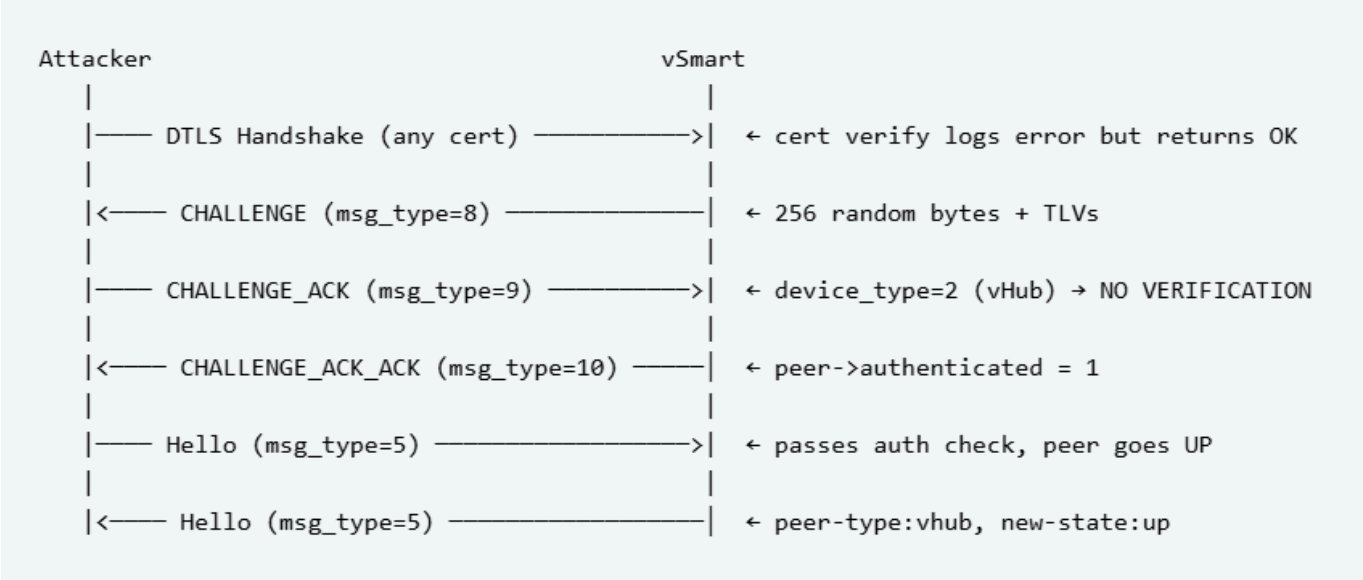
«Una vulnerabilidad en el mecanismo de autenticación entre pares de Cisco Catalyst SD-WAN Controller, anteriormente conocido como SD-WAN vSmart, y Cisco Catalyst SD-WAN Manager, antes llamado SD-WAN vManage, podría permitir que un atacante remoto no autenticado evada los controles de autenticación y obtenga privilegios administrativos en un sistema afectado», indicó Cisco.

La empresa explicó que el problema se origina por un fallo en el mecanismo de autenticación entre nodos, el cual podría ser explotado mediante el envío de solicitudes especialmente diseñadas al sistema vulnerable.

Una explotación exitosa permitiría al atacante iniciar sesión en Cisco Catalyst SD-WAN Controller utilizando una cuenta interna de alto privilegio, aunque sin acceso root, y posteriormente aprovechar dicho acceso para interactuar con NETCONF y alterar la configuración de red de la infraestructura SD-WAN.

La vulnerabilidad afecta a las siguientes implementaciones:

- On-Prem Deployment
- Cisco SD-WAN Cloud-Pro
- Cisco SD-WAN Cloud (Cisco Managed)
- Cisco SD-WAN for Government (FedRAMP)



De acuerdo con Rapid7, empresa que descubrió CVE-2026-20182, esta vulnerabilidad guarda similitudes con CVE-2026-20127 (CVSS 10.0), otra falla crítica de bypass de autenticación que impacta el mismo componente. Se cree que esta última ha sido explotada desde al menos 2023 por un actor de amenazas identificado como UAT-8616.

«Esta nueva vulnerabilidad de bypass de autenticación afecta al servicio 'vdaemon' sobre DTLS (puerto UDP 12346), el mismo servicio vulnerable en CVE-2026-20127», señalaron los investigadores de Rapid7, Jonah Burgess y Stephen Fewer. *«La nueva falla no representa una evasión del parche de CVE-2026-20127. Se trata de un problema distinto ubicado en una sección similar de la pila de red de 'vdaemon'.»*

Aun así, el resultado final es equivalente: un atacante remoto sin autenticación puede aprovechar CVE-2026-20182 para hacerse pasar por un par autenticado del dispositivo objetivo y ejecutar operaciones privilegiadas.

En su aviso de seguridad, Cisco confirmó que detectó *«una explotación limitada»* de esta vulnerabilidad durante mayo de 2026, instando a sus clientes a instalar las actualizaciones más recientes lo antes posible.

La compañía también advirtió que los sistemas Catalyst SD-WAN Controller accesibles desde internet y con puertos expuestos presentan un mayor riesgo de compromiso. Por ello, recomienda revisar el archivo «/var/log/auth.log» en busca de registros relacionados con *«Accepted publickey for vmanage-admin»* provenientes de direcciones IP desconocidas o no autorizadas.

Otro posible indicador de compromiso es la aparición de eventos sospechosos de emparejamiento en los registros, incluyendo conexiones no autorizadas realizadas en horarios inusuales, originadas desde direcciones IP desconocidas o asociadas a tipos de dispositivos que no coinciden con la arquitectura habitual del entorno.