# Boletín de alerta

**Boletín Nro.:** 77
**Fecha de publicación:** 26/09/2025
**Tema:** Alerta 2025-77 Vulnerabilidades críticas en productos Cisco
**Traffic Light Protocol (TLP):** White

## Producto(s) afectado(s):

Para la **CVE-2025-20352**

- **Cisco IOS e IOS XE** que tengan habilitado el protocolo SNMP (Simple Network Management Protocol)

*Se incluyen switches **Cisco Catalyst 9300** y **Meraki MS390** ejecutando **Meraki CS 17** o versiones anteriores, así como routers y otros dispositivos que ejecutan IOS/IOS XE.*

Para la **CVE-2025-20333**

- **Cisco Secure Firewall ASA (Adaptive Security Appliance)** y **Cisco Secure Firewall Threat Defense (FTD)** en versiones **ASA 9.16, 9.17, 9.18, 9.19, 9.20, 9.22, y FTD 7.0, 7.2, 7.4, 7.6**

## Descripción

Recientemente, el equipo de seguridad de **Cisco** reportó y publicó varias vulnerabilidades críticas como parte de un conjunto de actualizaciones. Identificadas bajo el **CVE-2025-20352**, la cual trata de un desbordamiento de pila en la implementación de **SNMP** dentro de IOS/IOS XE, que recibió una calificación de severidad alta con un puntaje **CVSS de 7.7**, además se publico la **CVE-2025-20333**, una zero-day que aparece como un fallo de validación incorrecta de entrada (input validation) en solicitudes HTTP(S), que permite a un atacante autenticado ejecutar código arbitrario con CVSS de 9.9 considerada de muy alta severidad.

La vulnerabilidad **CVE-2025-20352** puede ser aprovechada mediante el envío de paquetes SNMP especialmente diseñados sobre IPv4 o IPv6. Un atacante que cuente con la cadena “read-only community string” en SNMP v1/v2c o credenciales válidas en SNMP v3 puede provocar un **reinicio del dispositivo (denegación de servicio)**. Si, además, obtiene credenciales con privilegio de administración (nivel 15 en IOS XE), es posible escalar el ataque hasta lograr la **ejecución remota de código (RCE) como usuario root** en el sistema operativo del dispositivo, comprometiendo por completo su integridad. Cisco informó que los casos observados en explotación real ocurrieron tras el robo o compromiso de credenciales administrativas, lo que facilitó la ejecución del ataque.

Según Shodan a septiembre de 2025, en Mexico existe una exposición actual a esta vulnerabilidad de 453 panales Cisco ASA expuestos y 55852 a nivel mundial.


En la vulnerabilidad **CVE-2025-20333,** un atacante, con credenciales válidas para VPN WebVPN del dispositivo ASA/FTD, puede enviar solicitudes HTTP(S) malformadas al servidor web interno del dispositivo. Si tiene éxito, puede ejecutar código con privilegios root en el dispositivo afectado, comprometiendo completamente su seguridad. Adicionalmente, se han reportado técnicas de persistencia mediante manipulación del ROMMON en dispositivos comprometidos, siendo esta manipulación parte de la actividad observada, aunque no necesariamente parte directa de la explotación inicial del CVE.

Cisco confirmó que la falla **CVE-2025-20352 ya está siendo explotada activamente** en entornos reales, lo que incrementa el nivel de riesgo para organizaciones que aún no han aplicado las correcciones.

## Mitigación y solución:

Cisco ha publicado parches oficiales que corrigen ambas vulnerabilidades tanto para dispositivos en IOS e IOS XE como para ASA y FTD. La solución recomendada es actualizar los dispositivos afectados a versiones corregidas, como **IOS XE 17.15.4a o posteriores** en el caso de switches Catalyst y Meraki y versiones parcheadas de ASA y FTD.

Mientras la actualización no sea posible, se sugieren medidas de mitigación temporales:

- Restringir el acceso a SNMP únicamente a direcciones IP de redes confiables.
- Deshabilitar el OID vulnerable de SNMP si la configuración del dispositivo lo permite.
- Monitorizar los hosts SNMP configurados mediante el comando “show snmp host” para detectar accesos inesperados o no autorizados.
- Para ASA y FTD no se conocen mitigaciones “temporales” confiables o workarounds simples proporcionados por Cisco: la recomendación prioritaria es aplicar el parche cuanto antes.
- En entornos con sospecha de compromiso, es esencial recolectar volcados de memoria (memory dumps) y realizar análisis forense del estado del sistema, especialmente del proceso WebVPN y de la carga de módulos modificados en ROMMON si se sospecha persistencia.

- Tras la aplicación del parche, revisar logs históricos del WebVPN para peticiones malformadas, clientes VPN sospechosos y patrones de tráfico anómalos.
- Reforzar la segmentación de acceso VPN, políticas de acceso al portal WebVPN, y monitoreo continuo de actividades fuera de lo común.

Además, se recomienda reforzar la gestión de credenciales administrativas, asegurando contraseñas robustas, autenticación de múltiples factores en accesos remotos, y monitoreo activo de intentos de acceso sospechosos.

## Información adicional:

- Cisco fixes IOS/IOS XE zero-day exploited by attackers (CVE-2025-20352) – Help Net Security
- Cisco Warns of Actively Exploited SNMP Vulnerability Allowing RCE or DoS in IOS Software
- Cisco Patches Zero-Day Flaw Affecting Routers and Switches – SecurityWeek
- Cisco uncovers new SNMP vulnerability used in attacks on IOS devices | CyberScoop
- Cisco Event Response: Continued Attacks Against Cisco Firewalls
- CVE-2025-20333, CVE-2025-20362: Cisco Zero-Days Exploited | Tenable®
- Cisco Secure Firewall Adaptive Security Appliance Software and Secure Firewall Threat Defense Software VPN Web Server Remote Code Execution Vulnerability