Boletín de alerta

Boletín Nro.:
Fecha de publicación: 19/03/2026
Tema: Alerta 2026-28 Vulnerabilidades críticas en Cisco IOS XR
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- Software Cisco IOS XR:
  - Versiones 25.4.x anteriores a 25.4.2
  - Versiones 25.3.x (todas)
  - Versiones 7.8 hasta 25.2.21
- Routers Cisco IOS XRv 9000
- Plataformas de red como serie NCS 5700
- Infraestructura basada en IOS XR en entornos físicos y virtuales

Descripción

Se han identificado múltiples vulnerabilidades en **Cisco IOS XR** que podrían permitir a un atacante comprometer completamente los dispositivos de red:

- **CVE-2026-20040 (CVSS 8.8 – Alta):** Vulnerabilidad de inyección de comandos en la CLI. Un usuario autenticado con privilegios bajos puede ejecutar comandos arbitrarios como **root**, debido a una validación insuficiente de parámetros, comprometiendo el sistema operativo subyacente.
- **CVE-2026-20046 (CVSS 8.8 – Alta):** Falla en la asignación de privilegios dentro de la CLI. Permite a un atacante eludir controles de autorización y obtener **control administrativo total** del dispositivo.
- **CVE-2026-20074 (CVSS 7.4 – Alta):** Vulnerabilidad en el protocolo de enrutamiento **IS-IS**. Un atacante adyacente no autenticado puede enviar paquetes manipulados para reiniciar procesos críticos, causando **interrupciones de red (DoS)**.
- **CVE-2026-20118 (CVSS 6.8 – Media):** Vulnerabilidad en el manejo de interrupciones de tráfico (EPNI). Un atacante remoto no autenticado puede enviar tráfico especialmente diseñado para degradar o interrumpir el procesamiento, generando **pérdida de paquetes y denegación de servicio**.

En conjunto, estas vulnerabilidades pueden afectar la **confidencialidad, integridad y disponibilidad** de la infraestructura, permitiendo desde escalación de privilegios hasta interrupciones operativas críticas. Actualmente, **no se ha confirmado explotación activa**

Solución y mitigaciones:

- Actualizar inmediatamente a versiones corregidas de Cisco IOS XR.
- Aplicar los parches y SMU recomendados por el fabricante.

Información adicional:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-privesc-bF8D5U4W
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-isis-dos-kDMxpSzK
- https://www.euskadi.eus/gobierno-vasco/-/noticia/2026/actualizaciones-de-cisco-para-ios-xr/