

Boletín de alerta

Boletín Nro.: 120

Fecha de publicación: 22/10/2026

Tema: Alerta 2026-120 Vulnerabilidades críticas en Cisco Snort 3 afectan a FTD, Cyber Vision y otros productos

Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Producto

Open Source Snort 3

Cisco Secure Firewall Threat Defense (FTD)

UTD en Cisco IOS XE

Cisco Cyber Vision

Cisco Meraki MX

Cisco Cloud-delivered Firewall y Secure Access

Versiones afectadas

Anteriores a 3.12.4.0

Anteriores a 7.0.10, 7.2.12, 7.4.8, 7.6.6, 7.7.13 y 10.0.2

Anteriores a 17.12.8, 17.15.6, 17.18.5, 26.1.2 y 26.2.1

Anteriores a 5.6.0

Equipos sin el paquete Snort 3 actualizado

Actualizados por Cisco el 21/10/2026

Afectan independientemente de la configuración. Open Source Snort 2 no está afectado.

Descripción

Se ha publicado una vulnerabilidad crítica de escritura fuera de los límites de memoria (CWE-787) en el motor de inspección Snort 3 de Cisco, identificada como CVE-2026-20043 (CVSSv3.1 9.0 – CRÍTICO), que afecta a Open Source Snort 3 y a los productos de Cisco que lo integran, entre ellos Secure Firewall Threat Defense (FTD), Cyber Vision, Meraki MX, UTD en IOS XE, Cloud-delivered Firewall y Secure Access.

La falla se publicó el 21 de octubre de 2026 dentro de una versión de hardening (refuerzo de seguridad) de Snort 3, que corrige múltiples vulnerabilidades descubiertas por el propio equipo de ingeniería de Snort 3 durante una revisión interna. Cisco agrupó los fallos por clase de debilidad (CWE) y asignó un único CVE a cada grupo. La puntuación de cada CVE corresponde a la vulnerabilidad más grave de su grupo.

El vector de CVE-2026-20043 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H) indica que se puede explotar por red, sin autenticación ni interacción del usuario, aunque con complejidad alta. Un ataque exitoso podría comprometer la confidencialidad, la integridad y la disponibilidad, con alcance más allá del componente vulnerable. Cisco no describe los componentes concretos de Snort 3 afectados ni las

condiciones técnicas de explotación.

El mismo aviso incluye otras tres agrupaciones de vulnerabilidades:

CVE	CVSS máximo (aviso de Cisco)	CWE	Clase de vulnerabilidad
CVE-2026-20043	9.0	CWE-787	Escritura fuera de límites
CVE-2026-20236	9.0	CWE-682	Cálculo incorrecto
CVE-2026-20291	7.8 (vector local, requiere privilegios bajos)	CWE-269	Gestión inadecuada de privilegios
CVE-2026-20356	7.5	CWE-400	Consumo de recursos no controlado (denegación de servicio)

Cisco PSIRT no tiene conocimiento de anuncios públicos ni de explotación maliciosa de estas vulnerabilidades. Según el fabricante, se descubrieron en pruebas internas de seguridad que combinaron los procesos de prueba existentes con modelos de IA de frontera.

Solución

Cisco recomienda actualizar a las versiones corregidas de cada producto e indica que no hay workarounds que eviten estas vulnerabilidades. Por su función de inspección de tráfico, se recomienda priorizar los equipos perimetrales (FTD, UTD en routers IOS XE) y los sensores Snort 3 autogestionados.

Cisco Secure Firewall Threat Defense (FTD)

Rama de Cisco Secure FTD Primera versión corregida

7.0 y anteriores	7.0.10
7.2	7.2.12
7.4	7.4.8
7.6	7.6.6
7.7	7.7.13
10.0	10.0.2
10.1	10.1.0

Unified Threat Defense (UTD) en Cisco IOS XE

Las siguientes imágenes UTD de Cisco IOS XE incluyen Open Source Snort 3 versión 3.12.4.0 (tabla actualizada por Cisco el 22/10/2026, versión 1.1 del aviso):

Rama de Cisco IOS XE Primera versión corregida (imagen UTD)

17.12	17.12.8 (secapp-utd.17.12.08.1.2.8_SV3.12.4.0_XE17.12)
-------	--

17.15	17.15.6 (secapp-utd.17.15.06.1.0.21_SV3.12.4.0_XE17.15)
17.18	17.18.5
26.1	26.1.2 (secapp-utd.26.01.02.1.0.6_SV3.12.4.0_XE26.1)
26.2	26.2.1

Open Source Snort 3, Cyber Vision y servicios gestionados

Producto	Rama	Acción / versión corregida
Open Source Snort 3	3.x	Actualizar a 3.12.4.0
Cisco Cyber Vision	Anteriores a 5.6	Migrar a una versión corregida
Cisco Cyber Vision	5.6	5.6.0
Cisco Meraki MX	—	Sin acción: Cisco actualizó automáticamente el paquete Snort 3 el 21/10/2026 en los equipos en línea y conectados a Meraki Dashboard
Cisco CDFW y CSA	—	Sin acción: instancias en la nube actualizadas por Cisco el 21/10/2026

Para Meraki MX, se recomienda comprobar en Meraki Dashboard que no queden equipos desconectados o fuera de línea que no hayan recibido el paquete Snort 3 corregido.

Guías de actualización de Cisco Secure Firewall Threat Defense / Management Center:

<https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-guides-list.html>

Versión 3.12.4.0 de Open Source Snort 3:

<https://github.com/snort3/snort3/releases/tag/3.12.4.0>

Información adicional:

- Cisco PSIRT — Multiple Cisco Products Snort 3 Security Hardening Release: October 2026: <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-snort3-ybgmhTQe>
- Cisco PSIRT — notificación anticipada de los avisos del 21 de octubre de 2026 (avisos relacionados de Snort 3): <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-notice-QGwHnJ6k>
- NVD — CVE-2026-20043: <https://nvd.nist.gov/vuln/detail/CVE-2026-20043>
- NVD — CVE-2026-20236: <https://nvd.nist.gov/vuln/detail/CVE-2026-20236>
- NHS England Digital — CC-4878, Cisco Releases Security Hardening Guidance for Multiple Cisco Products: <https://digital.nhs.uk/cyber-alerts/2026/cc-4878>

- Snort 3 — release 3.12.4.0 (GitHub):
<https://github.com/snort3/snort3/releases/tag/3.12.4.0>