Incidente ID:	0023
Fecha del reporte:	08/01/2026
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Vulnerabilidad en SNORT 3 de Cisco
Herramienta de detección	N/A
Activo involucrado:	SNORT 3
Tipo de incidente:	Boletín informativo
Nivel de riesgo:	Alto

Objetivo:

Informar a las entidades del Ecosistema Digital sobre las vulnerabilidades encontradas en el sistema de prevención y detección de intrusiones (IDS/IPS) SNORT 3 de Cisco, las vulnerabilidades fueron reportadas con los códigos CVE-2026-20026 (CVSS: 5.8) y CVE-2026-20027 (CVSS: 5.3)

Descripción:

Se han divulgado dos vulnerabilidades de seguridad significativas que afectan al motor de detección Cisco Snort 3. Estas fallas residen en el procesamiento del protocolo DCE/RPC (Distributed Computing Environment / Remote Procedure Call) y permiten a un atacante remoto no autenticado comprometer la disponibilidad del servicio o acceder a información sensible.

- CVE-2026-20026 (Denegación de Servicio - DoS):

– Descripción: Vulnerabilidad de "Use-After-Free" (uso de memoria después de su liberación).

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- Impacto: Permite que el motor de detección Snort 3 se reinicie inesperadamente, interrumpiendo la inspección de tráfico y provocando una condición de denegación de servicio.

- CVE-2026-20027 (Divulgación de Información):

- Descripción: Vulnerabilidad de "Out-of-Bounds Read" (lectura fuera de los límites).

- Impacto: Permite a un atacante leer memoria adyacente a los búferes asignados, lo que podría resultar en la fuga de información sensible del flujo de datos procesado por Snort.

Las vulnerabilidades afectan al software Cisco Secure Firewall Threat Defense, al software de código abierto Snort 3, al software Cisco IOS XE con capacidades Unified Threat Defense y a varios dispositivos Cisco Meraki.

Las organizaciones que ejecutan Snort 3 en nuevas instalaciones de Cisco Secure FTD versiones 7.0.0 y posteriores son particularmente vulnerables, ya que Snort 3 funciona de forma predeterminada en estas versiones.

La superficie de ataque sigue siendo extensa dada la implementación generalizada de Snort 3 en redes empresariales de todo el mundo.

Productos afectados:

La vulnerabilidad afecta a cualquier producto de Cisco o de código abierto que utilice el motor de detección Snort 3. Esto incluye, pero no se limita a:

- Cisco Secure Firewall Threat Defense (FTD): Versiones 7.0.0 y posteriores (donde Snort 3 es el motor por defecto).

- Cisco IOS XE Software: Dispositivos que ejecutan la funcionalidad Unified Threat Defense (UTD).

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- 1000 Series Integrated Services Routers (ISRs)
- 4000 Series ISRs
- Catalyst 8000V Edge Software
- Catalyst 8200 Series Edge Platforms
- Catalyst 8300 Series Edge Platforms
- Catalyst 8500L Edge Platforms
- Cloud Services Routers 1000V
- Integrated Services Virtual Routers

- Cisco Meraki MX: Dispositivos de seguridad y SD-WAN que utilizan el motor de prevención de intrusiones basado en Snort.

- MX67
- MX67C
- MX67W
- MX68
- MX68CW
- MX68W
- MX75
- MX84
- MX85
- MX95
- MX100
- MX105
- MX250
- MX400
- MX450
- MX600
- MX Z4
- MX vMX

- Snort 3 (Open Source): Versiones anteriores a la 3.9.6.0.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Nota: Los productos que utilizan exclusivamente el motor Snort 2 no están afectados por estas vulnerabilidades específicas.

Modo de explotación y cadena de infección

Vector de Ataque: Red (Remoto). No requiere autenticación ni interacción del usuario.

Procedimiento: Un atacante envía un gran volumen de peticiones DCE/RPC especialmente manipuladas a través de una conexión establecida que esté siendo inspeccionada por Snort 3.

Ejecución del Fallo:

En el caso del CVE-2026-20026, la lógica de manejo de búfer falla, intentando acceder a una dirección de memoria que ya ha sido liberada (*free*), lo que fuerza al proceso del motor a colapsar y reiniciarse.

En el caso del CVE-2026-20027, la validación incorrecta permite al proceso leer datos más allá del final del búfer asignado, devolviendo datos residuales de la memoria que pueden contener paquetes de otros usuarios o credenciales.

Recomendaciones de mitigación:

- Aplicar las respectivas actualizaciones

– Snort 3 Open Source: Actualizar inmediatamente a la versión 3.9.6.0 o superior.

– Cisco Secure Firewall (FTD): Instalar los *Hot Fixes* disponibles para las versiones 7.0, 7.2 y superiores según el portal de soporte de Cisco.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

– Cisco IOS XE / Meraki: Verificar la disponibilidad de parches en el panel de administración (Cisco ha programado liberaciones progresivas hasta febrero de 2026 para algunas plataformas; monitorear avisos del proveedor).

- Determinar si UTD está habilitado

Para determinar si UTD está habilitado en un dispositivo, utilice el comando show utd engine standard status. Si el resultado muestra " Sí" en "En ejecución", UTD está habilitado. Si no hay ningún resultado, el dispositivo no se ve afectado. El siguiente ejemplo muestra el resultado en un dispositivo con UTD habilitado:

```
Router# show utd engine standard status
Engine version        : 1.0.19_SV2.9.16.1_XE17.3
Profile               : Cloud-Low
System memory         :
             Usage    : 6.00 %
             Status   : Green
Number of engines     : 1

Engine         Running    Health     Reason
=======================================
Engine(#1):    Yes        Green      None
=======================================================
```


CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Fuentes:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort3-dcerpc-vulns-J9HNF4tH
- https://cybersecuritynews.com/cisco-snort-3-detection-engine-vulnerability/
- https://www.ccn-cert.cni.es/es/seguridad-al-dia/vulnerabilidades/view/35095.html
- https://www.cve.org/CVERecord?id=CVE-2026-20026
- https://www.google.com/search?q=https://www.cve.org/CVERecord%3Fid%3DCVE-2026-20027
- https://www.snort.org/downloads/#snort-3.0

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas telefónicas (+57) 316 8931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570