Vulnerabilidades en Cisco NX-OS

CYBERZAINTZA-AVISOS

TLP: CLEAR

www.ciberseguridad.eus

EUSKO JAURLARITZA
GOBIERNO VASCO

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que la Agencia de Ciberseguridad Vasca considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso la Agencia de Ciberseguridad Vasca puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de la Agencia de Ciberseguridad Vasca como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de la Agencia de Ciberseguridad Vasca. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

1. Resumen ejecutivo

Cisco ha publicado avisos de seguridad para tratar **2 vulnerabilidades**, de **severidad alta**, que afectan al producto **Cisco NX-OS**, el sistema operativo de centro de datos del fabricante, con los identificadores CVE-2024-20321 y CVE-2024-20267. Estas vulnerabilidades suponen una amenaza de alta gravedad para productos de Cisco con impacto en la disponibilidad de los sistemas que se vean afectados.

Por otra parte, el Equipo de Respuesta a Incidentes de Seguridad de Productos de Cisco (PSIRT) no tiene conocimiento de divulgación o uso malicioso de las vulnerabilidades descritas.

El fabricante ya ha publicado las actualizaciones y medidas de mitigación correspondientes, corrigiendo de esta manera los fallos destacados. Por lo que, para prevenir estas y otras vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen los parches correspondientes.

2. Recursos afectados

La primera vulnerabilidad publicada, cuyo identificador es CVE-2024-20321, afecta a los switches de la serie Nexus 3600 y a las tarjetas de línea de la serie Nexus 9500 R con los siguientes indicadores:

- N3K-C36180YC-R
- N3K-C3636C-R
- N9K-X9624D-R2
- N9K-X9636C-R
- N9K-X9636C-RX
- N9K-X9636Q-R
- N9K-X96136YC-R

La segunda vulnerabilidad publicada, cuyo identificador es CVE-2024-20267, afecta a los siguientes productos si están ejecutando una versión vulnerable del software Cisco NX-OS y tienen configurado MPLS:

- Switches de la serie Nexus 3000.
- Switches de la plataforma Nexus 5500.
- Switches de la plataforma Nexus 5600.
- Switches de la serie Nexus 6000.
- Switches de la serie Nexus 7000.
- Switches de la serie Nexus 9000 con NX-OS en modo “standalone”.

3. Análisis técnico

Los detalles de las vulnerabilidades tratadas en este aviso son los siguientes:

CVE-2024-20321: vulnerabilidad de denegación de servicio que afecta a la implementación del protocolo eBGP (External Border Gateway Protocol) en Cisco NX-OS. La causa de esta vulnerabilidad tiene su origen en cómo se gestiona el tráfico de eBGP que está asignado a una cola de limitación de velocidad de hardware compartida. Un atacante podría explotar esta vulnerabilidad enviando grandes cantidades de tráfico de red con ciertas características a través de un dispositivo afectado causando una condición de denegación de servicio DoS en la red.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE-400: Uncontrolled Resource Consumption

CVSS Base: **8.6**

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: **Con cambios**
- **Confidencialidad:** Ninguna
- **Integridad:** Ninguna
- **Disponibilidad: Alta**

CVE-2024-20267: vulnerabilidad de denegación de servicio que afecta al manejo del tráfico en Cisco NX-OS cuyo origen radica en la falta de verificación de errores al procesar un marco MPLS de ingreso. Un atacante remoto podría explotar esta vulnerabilidad mediante el envío de un paquete Ipv6 manipulado que esté encapsulado dentro de un marco MPLS a una interfaz habilitada para MPLS del dispositivo objetivo. La explotación exitosa conduciría a una condición de denegación de servicio DoS.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE-120: Buffer Copy without Checking Size of Input

CVSS Base: **8.6**

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ningunos**

- **Interacción con el usuario**: **Ninguna**
- **Alcance**: **Con cambios**
- **Confidencialidad:** Ninguna
- **Integridad:** Ninguna
- **Disponibilidad: Alta**

4. Mitigación / Solución

Cisco ha lanzado actualizaciones de software gratuitas que abordan las vulnerabilidades descritas en este aviso. Los clientes con contratos de servicio que les otorgan actualizaciones regulares de software deben obtener correcciones de seguridad a través de sus canales de actualización habituales.

5. Referencias Adicionales

- Avisos de seguridad.
- CVE-2024-20321.
- CVE-2024-20267.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY