Basque CyberSecurity Centre

Vulnerabilidad en software Cisco IOS XR para enrutadores ASR 9000

BCSC-AVISOS

TLP: CLEAR

www.ciberseguridad.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

TABLA DE CONTENIDO

Sobre el BCSC 3
1. Aviso de seguridad 4
2. Recursos afectados 5
3. Análisis técnico 6
4. Mitigación / Solución 7
5. Referencias Adicionales 8

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC 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 BCSC 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 BCSC. 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.

Sobre el BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.

El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

FIRST Improving Security Together
TF-CSIRT Trusted Introducer
CSIRT.es

1. Aviso de seguridad

Cisco ha hecho público un nuevo aviso de seguridad donde se corrige una vulnerabilidad de severidad alta que afecta al software Cisco IOS XR para enrutadores Cisco ASR 9000 Series Aggregation Services Routers, ASR 9902 Compact High-Performance Routers y ASR 9903 Compact High-Performance Routers. El identificador de este fallo es CVE-2023-20049 que tras una explotación exitosa, puede conducir a una condición de denegación de servicio afectando a la disponibilidad de los sistemas afectados. Cabe destacar que desde Cisco PSIRT se informa de no tener conocimiento de ningún anuncio público o uso malintencionado de la vulnerabilidad descrita.

El fabricante ya ha publicado las actualizaciones correspondientes, corrigiendo de esta manera el fallo destacado.

2. Recursos afectados

- Esta vulnerabilidad afecta a productos de Cisco que están ejecutando una versión vulnerable del software Cisco IOS XR de 64 bits y tienen habilitada la descarga de hardware BFD para cualquiera de las tarjetas de línea instaladas, que son:
  - Series Aggregation Services Routers de la serie ASR 9000 solo si tienen instalada una tarjeta de línea basada en Lightspeed o Lightspeed Plus.
  - ASR 9902 Compact High-Performance Routers.
  - ASR 9903 Compact High-Performance Routers.

3. Análisis técnico

Los detalles de la vulnerabilidad tratada en esta actualización son los siguientes:

CVE-2023-20049: vulnerabilidad de denegación de servicio debido al incorrecto tratamiento de los paquetes BFD con formato erróneo y que son recibidos en tarjetas en línea donde está habilitada la característica de descarga de hardware BFD, de forma que, un atacante podría aprovechar esta vulnerabilidad si envía un paquete BFD IPv4 diseñado a un dispositivo afectado. Un exploit exitoso podría permitir al atacante causar excepciones de tarjeta de línea o un restablecimiento completo, lo que resultaría en la pérdida de tráfico sobre esa tarjeta de línea mientras se recarga.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 8.6, Alta

VSS: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

Para la mitigación de estas vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen las actualizaciones correspondientes.

Para la mitigación de esta vulnerabilidad Cisco ha lanzado la actualización de software que la corrige a través de los canales de actualización habituales para sus clientes, existiendo workaround para su mitigación que se puede consultar en el propio aviso.

.

5. Referencias Adicionales

- Aviso de seguridad.
- CVE-2023-20049.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA