I. DATOS GENERALES:

Clase de alerta: Incidente

Tipo de incidente: DoS (Denied of Service)

Nivel de riesgo: Alto

II. ALERTA

Cisco corrigió una vulnerabilidad DoS de alta gravedad (CVE-2023-20049) en el software IOS XR que afecta a varios enrutadores empresariales.

Cisco lanzó actualizaciones de seguridad para abordar una vulnerabilidad DoS de alta gravedad, rastreada como CVE-2023-20049 (puntaje CVSS de 8.6), en el software IOS XR utilizado por varios enrutadores de nivel empresarial.

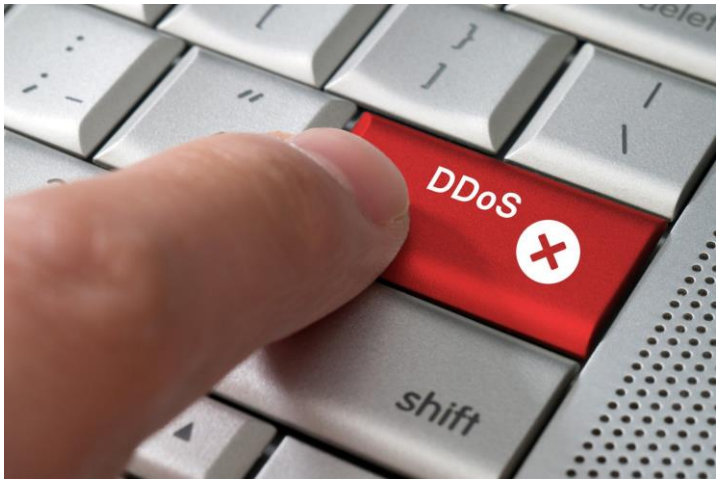

Figura 1.- lustraciones distintivas de DoS (Blackcat)
Fuente: BleepingComputer

III. INTRODUCCIÓN

La vulnerabilidad reside en la función de descarga de hardware de detección de reenvío bidireccional (BFD) del software Cisco IOS XR para enrutadores de servicios de agregación de la serie Cisco ASR 9000, enrutadores compactos de alto rendimiento ASR 9902 y enrutadores compactos de alto rendimiento ASR 9903.

Un atacante remoto no autenticado puede activar la falla para hacer que una tarjeta de línea se reinicie, lo que resulta en una condición de denegación de servicio (DoS).

“Esta vulnerabilidad se debe al manejo incorrecto de paquetes BFD con formato incorrecto que se reciben en tarjetas de línea donde está habilitada la función de descarga de hardware BFD”. Una explotación exitosa podría permitir que el atacante provoque excepciones en la tarjeta de línea o un restablecimiento completo, lo que resultaría en la pérdida de tráfico en esa tarjeta de línea mientras se recarga la tarjeta de línea”.

Esta falla afecta a los enrutadores Cisco que ejecutan 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.

Los enrutadores de servicios de agregación de la serie ASR 9000 solo si tienen instalada una tarjeta de línea basada en Lightspeed o Lightspeed-Plus

Enrutadores compactos de alto rendimiento ASR 9902

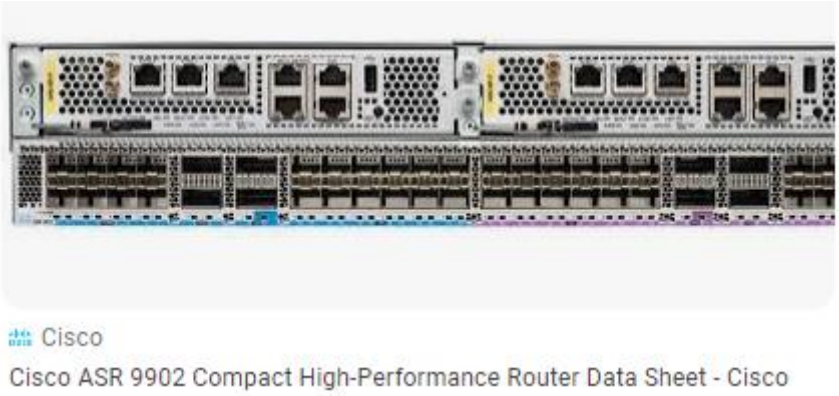

Figura 2.- ***Router Cisco ASR 9902***

Enrutadores compactos de alto rendimiento ASR 9903

Figura 2.- ***Router Cisco ASR 9902***

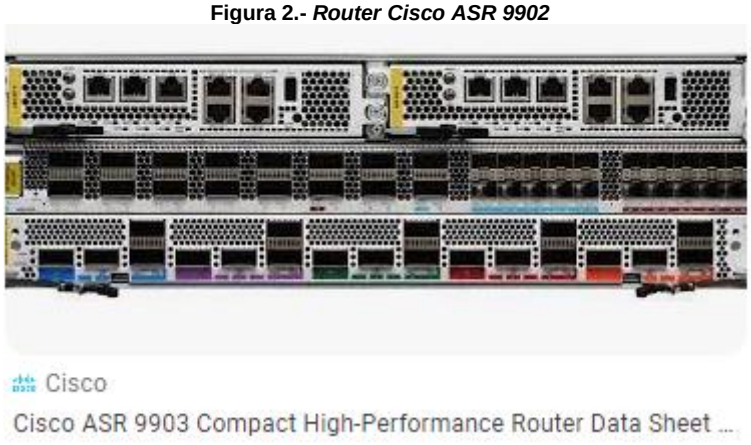

Figura 3.- ***Router Cisco ASR 9903***

La empresa señaló que esta vulnerabilidad no afecta a los siguientes productos de Cisco:

- Software del IOS
- Software IOS XE
- Plataformas IOS XR no enumeradas en la sección Productos vulnerables de este aviso

Como solución alternativa, Cisco recomienda deshabilitar la descarga de hardware BFD y crear listas de control de acceso a la infraestructura.

El gigante de TI abordó el problema con el lanzamiento de las versiones 7.5.3, 7.6.2 y 7.7.1 de IOS XR.

IV. VECTOR DE ATAQUE:

También conocido como DDoS, el ataque de denegación de servicio -DoS- consiste en un incidente cuya principal finalidad es dejar indisponible un sitio *web* o recurso de red.

Para eso, el individuo o grupo malicioso genera una sobrecarga en el blanco mediante un tráfico de internet indeseado o el agotamiento de los recursos de computación del activo. Así pues, mitiga la probabilidad que tráfico normal alcance su destino.

Básicamente, en este tipo de ataque a una aplicación web, red, a las APIs o a una infraestructura de data center, el malintencionado tiene como reto ocasionar una gran pérdida como:

- Inactivar el sistema
- Limitar o impedir que usuarios registrados accedan al ambiente para realizar tareas relevantes como buscar información
- Efectuar compras
- Cerrar negocios

Durante un ataque de este tipo, los invasores utilizan muchas máquinas y dispositivos conectados a internet incluyendo elementos de Internet de las Cosas, ordenadoras personales, dispositivos móviles y servidores de red para enviar un gran volumen de tráfico a sus blancos.

V. IMPACTO:

De acuerdo con una investigación realizada por Gartner, se estima que el impacto financiero inherente a los ataques a sistemas ciberfísicos alcanzará los USD 50 billones hasta el 2023. Esto significa que, a medida que la tecnología avanza, las amenazas de ciberseguridad se vuelven cada vez más sofisticadas colocando en riesgo y en evidencia los datos sigilosos de las organizaciones, y entre estas encontramos los ataques de denegación de servicio.

VI. INDICADORES DE COMPROMISO

VII. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

Luego de conocer qué es un **ataque de denegación de servicio** y entender cómo puede afectar la seguridad de la información de los negocios modernos, es hora de hacer hincapié en la apuesta de las empresas a la ciberseguridad en México abordando las maneras más efectivas de prevenir y encarar este tipo de ataque.

1. Reconocer la fuente del ataque

Al reconocer el IP de los ordenadores afectados, puedes hacer una lista de control en el firewall del servidor para bloquear su acceso. Incluso, es recomendable que alteres la dirección de IP del servidor durante un cierto tiempo. Sin embargo, si el *usuario malicio* descubre la IP recién configurada, esta solución puede perder su eficacia.

2. Bloquea el IP del país

En el caso que detectes el origen del ataque desde un determinado país, es interesante que bloquees su IP mediante mecanismos automatizados que permitan mitigar de manera temprana un posible impacto.

3. Monitorea el tráfico a tu red

Conocer quién ingresa a tu red y asegurar que solamente usuarios registrados puedan acceder a la información son aspectos que debes poner en primer plano. El control de la actividad en la red corporativa permite detectar ataques en menor escala antes de que abran espacio para la generación de un gran evento.

4. Controla las vulnerabilidades

Es imperativo contar con tecnologías que habiliten la identificación de vulnerabilidades en los equipos y riesgos en la infraestructura que puedan poner en peligro la integridad del sistema y de la red, así como la confidencialidad de la información, para evitar que se tome ventaja del sistema afectado en este tipo de ataques de negación de servicio y pueden servir de puente para amplificar dichos eventos.

5. Prioriza la protección de *Endpoint*

Al contar con una solución de ciberseguridad de primera calidad, la empresa puede poner en marcha un análisis continuo de los archivos con el afán de prevenir y detectar amenazas que impacten la idoneidad de los documentos corporativos y que se pueda evitar que formen parte de una red conocida como BotNet.

VIII. DESCARGO DE RESPONSABILIDAD

La información en la presente alerta; se proporciona con fines informativos.

Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.

La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

- https://securityaffairs.com/143366/security/cisco-cve-2023-20049-dos.html
- https://www.ikusi.com/mx/blog/como-prevenir-los-ataques-de-denegacion-de-servicio/
- https://csirt.telconet.net/comunicacion/noticias-seguridad/vulnerabilidad-en-routers-cisco-ios-xr/#:~:text=La%20vulnerabilidad%20identificada%20como%20CVE,de%20forma%20remota%2C%20sin%20autenticaci%C3%B3n.