CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Vulnerabilidad de software

Fecha: 14/09/2023

Problemática: Cisco VPN Routers presentó fallas de consideración

Correlativo: AC-0068

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

Múltiples vulnerabilidades en soluciones Cisco VPN Routers podrían permitir a un atacante acceder a una instancia afectada sin limitaciones de seguridad.

SITUACIÓN

Routers afectados son vulnerables a los ataques si se ejecuta una versión de firmware anterior a la versión 1.0.01.02. Las fallas en la interfaz de administración del router, podrían propiciar que un atacante remoto autenticado ejecute un código arbitrario, provocando una denegación de servicio.

Los recursos que se ven afectados se encuentran los modelos;

- RV110W
- RV130W
- RV215W
- VPN RV160
- RV260
- RV260P
- RV260W

Nivel de priorización

Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
Urgente	**Preventiva**

Matriz de Evaluación

Riesgo Alto/ Medio/ Bajo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
Alto	**Alto**	**Alta**	**Alta**

RECOMENDACIONES

Ante esta alerta se dan las siguientes recomendaciones para mitigar este tipo de ataques:

- Aplique las actualizaciones emitidas por el fabricante
- Asegúrese de que todo el tráfico cableado y/o inalámbrico esté encriptado adecuadamente.
- Utilice dispositivos de red y software de seguridad basado en host para bloquear el tráfico de red que no es necesario dentro del entorno
- Limite el acceso a la infraestructura de red y los recursos que se pueden usar para remodelar el tráfico o producir condiciones AiTM.
- Los sistemas de detección y prevención de intrusiones en la red que pueden identificar patrones de tráfico indicativos

DICCIONARIO DE DATOS

- Atacante (ciberdelincuente, actor de amenazas): Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo, filtrado de información.
- Ciberataque: Intento deliberado de un ciberdelincuente de obtener acceso a un sistema informático sin autorización sirviéndose de diferentes tácticas y técnicas.

REFERENCIAS

CISCO
https://sec.cloudapps.cisco.com/security/center/publicationListing.x?product=Cisco&impac=critical&sort=-day_sir#~Vulnerabilities