Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA22-00557-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de enero de 2022
Última revisión	21 de enero de 2022

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT de Gobierno, comparte información sobre múltiples vulnerabilidades en Cisco Snort Modbus Denial of Service Vulnerability.

Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

Vulnerabilidades

CVE-2022-20685

Impactos

Vulnerabilidad de riesgo crítico

CVE-2022-20649: Una vulnerabilidad en el preprocesador Modbus del motor de detección de Snort podría permitir que un atacante remoto no autenticado provoque una condición de denegación de servicio (DoS) en un dispositivo afectado.

Productos afectados

Esta vulnerabilidad afecta a todas las versiones del proyecto Snort de código abierto anteriores a la versión 2.9.18 y la versión 3.1.0.100.

La vulnerabilidad afecta a los siguientes productos de Cisco si ejecutan una versión vulnerable del software de Cisco:

- Software de cibervisión
- Software Firepower Threat Defense (FTD) - Todas las plataformas
- Software de la serie Meraki MX

Esta vulnerabilidad afecta a los siguientes productos de Cisco si ejecutan una versión anterior a la primera versión corregida de Cisco Unified Threat Defense (UTD) Snort Intrusion Prevention System (IPS) Engine para Cisco IOS XE Software o Cisco UTD Engine para Cisco IOS XE SD- Software WAN:

- Enrutadores de servicios integrados (ISR) de la serie 1000
- Enrutadores de servicios integrados (ISR) de la serie 4000
- Software de borde Catalyst 8000V
- Plataformas perimetrales de la serie Catalyst 8200
- Plataformas perimetrales de la serie Catalyst 8300
- Plataformas perimetrales de la serie Catalyst 8500
- Plataformas perimetrales de la serie Catalyst 8500L
- Enrutadores de servicios en la nube 1000V
- Enrutadores virtuales de servicios integrados (ISRv)

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-dos-9D3hJLuj
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20649
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20648

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.01.21 09:41:41 -03'00'