Alerta de seguridad cibernética	9VSA21-00515-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de octubre de 2021
Última revisión	29 de octubre de 2021

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 una nueva vulnerabilidad en Cisco Firepower Threat Defense (FTD).

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

Vulnerabilidades

CVE-2021-34781

Impactos

CVE-2021-34781: Esta vulnerabilidad en el procesamiento de conexiones SSH para despliegues multi-instance de Cisco Firepower Threat Defense podría permitir a un atacante remoto no autenticado provocar una condición de denegación de servicio (DoS) en el aparato afectado. Esta vulnerabilidad se debe a una falta de un adecuado manejo de los errores cuando una sesión SSH falla en ser establecida.

Productos Afectados

Aparatos con una versión del software Cisco FTD vulnerable configurada para operación multi-instance, introducida en Cisco FTD Software 6.3.0. Las únicas plataformas de software Cisco FTD que permiten la operación multi-instance son: Firepower 4100 y Firepower 9300 Security Appliances.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-dos-rUDseW3r#vp

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34781

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.10.29 10:19:27 -03'00'