Alerta de seguridad cibernética	9VSA23-00946-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	21 de diciembre de 2023
Última revisión	21 de diciembre de 2023

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 CSIRT de Gobierno. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El CSIRT de Gobierno comparte información sobre vulnerabilidades que son parchadas en la versión 9.6 de OpenSSH.

Vulnerabilidades

CVE-2023-48795
CVE-2023-51385

Impacto

Vulnerabilidades de riesgo alto:

CVE-2023-48795: El protocolo de transporte SSH en ciertas extensiones OpenSSH, que se encuentra en versiones OpenSSH anteriores a la 9.6 y otros productos, permite a atacantes remotos evadir chequeos de integridad.

CVE-2023-51385: En SSH en OpenSSH anteriores a 9.6 puede ocurrir inyección de comandos OS si un nombre de usuario o de host tiene metacaracteres de shell, y este nombre es referenciado por un token de expansión en ciertas situaciones.

Mitigación

Instalar OpenSSH 9.6, el que se descarga en algunos de los mirrors listados aquí: https://www.openssh.com/ftp.html

Productos afectados

OpenSSH anteriores a 9.6.

Enlaces

https://www.openssh.com/txt/release-9.6

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.12.21 17:15:20 -03'00'