Alerta de seguridad cibernética	9VSA23-00783-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de febrero de 2023
Última revisión	6 de febrero 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 una nueva vulnerabilidad que afecta a OpenSSH server (SSHD), y para resolver la cual la empresa ha hecho disponible una actualización.

Vulnerabilidades

CVE-2023-25136

Impacto

Vulnerabilidades de riesgo crítico

CVE-2023-25136: OpenSSH server (sshd) 9.1 introdujo una vulnerabilidad double-free durante el manejo de los algoritmos options kex. Los descubridores de la vulnerabilidad señalan que “explotar esta vulnerabilidad no será fácil”.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

OpenSSH 9.1

Enlaces

https://nvd.nist.gov/vuln/detail/CVE-2023-25136
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25136

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.02.06 12:20:30 -03'00'

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

https://www.csirt.gob.cl
Teléfonos: 1510 | + (562) 24863850 | Correo: soc-csirt@interior.gob.cl
@csirtgob
https://www.linkedin.com/company/csirt-gob