Alerta de seguridad cibernética	9VSA21-00483-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de agosto de 2021
Última revisión	25 de agosto 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 vulnerabilidades en OpenSSL.

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

Vulnerabilidades

CVE-2021-3711
CVE-2021-3712

Impactos

CVE-2021-3711: Considerada de riesgo alto, esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el sistema objetivo.

CVE-2021-3712: Considerada de riesgo medio, esta vulnerabilidad permite a un atacante remoto acceder a inforomación potencialmente sensible.

Productos Afectados

OpenSSL de 1.0.2 a 1.1.1k

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://www.openssl.org/news/secadv/20210824.txt
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3711
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3712