# Alerta de Seguridad Cibernética

| | |
|---|---|
| Alerta de seguridad cibernética | 9VSA21-00539-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 29 de diciembre de 2021 |
| Última revisión | 29 de diciembre 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 dada a conocer para Apache LogJ4.

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

## Vulnerabilidad

CVE-2021-44832

## Impactos

CVE-2021-44832: Esta vulnerabilidad puede permitir la ejecución arbitraria de código y es considerada de riesgo medio, por ser más compleja de explotar que en el caso de la CVE-2021-44228 original (Véase: csirt.gob.cl/vulnerabilidades/9vsa21-00531-01/). Es parchada con la versión 2.17.1.

### Productos afectados

Apache Log4j2 2.0-beta7 a 2.17.0, exceptuando 2.3.2 y 2.12.4.

### Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.12.29 11:07:46 -03'00'

### Enlaces

https://logging.apache.org/log4j/2.x/security.html
https://checkmarx.com/blog/cve-2021-44832-apache-log4j-2-17-0-arbitrary-code-execution-via-jdbcappender-datasource-element/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44832