

# Alerta de Seguridad Cibernética

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno  
Ministerio del Interior y Seguridad Pública  
Gobierno de Chile



Alerta de seguridad cibernética	9VSA23-00763-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de enero de 2023
Última revisión	5 de enero 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 afectada a actualizaciones.

## Resumen

El CSIRT de Gobierno comparte la información sobre una nueva vulnerabilidad informada por Zoho para sus programas Access Manager Plus, PAM360 y Password Manager Pro.

## Vulnerabilidades

CVE-2022-47523

## Impacto

### Vulnerabilidades de riesgo crítico

**CVE-2022-47523:** Vulnerabilidad de inyección SQL.

### Productos afectados

Access Manager Plus 12200 y anteriores.  
PAM360 5800 y anteriores,  
Password Manager Pro 4308 y anteriores.

### Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

### Enlaces

<https://www.manageengine.com/privileged-session-management/advisory/cve-2022-47523.html>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-47523>

## 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://twitter.com/csirtgob)  
<https://www.linkedin.com/company/csirt-gob>