

Alerta de Seguridad Cibernética

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



Alerta de seguridad cibernética	9VSA23-00892-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	7 de septiembre de 2023
Última revisión	7 de septiembre 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 información sobre vulnerabilidades parchadas en la más reciente actualización de Apache SuperSet (versión 2.1.1).

Vulnerabilidades

CVE-2023-39265
CVE-2023-37941
CVE-2023-36388
CVE-2023-30776

Impacto

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

Apache Superset.

Enlaces

<https://github.com/apache/superset>
<https://downloads.apache.org/superset/2.1.1/>
<https://www.horizon3.ai/apache-superset-part-ii-rce-credential-harvesting-and-more/>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-39265>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-37941>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-36388>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-30776>