

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	9VSA24-00971-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	5 de febrero de 2024
Última revisión	5 de febrero de 2024

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 de una vulnerabilidad crítica en Mastodon.

Vulnerabilidades

[CVE-2024-23832](#)

Impacto

Vulnerabilidades de riesgo crítico:

CVE-2024-23832: Error de validación de origen. Permite a un atacante acceder a cualquier funcionalidad que sea inadvertidamente accesible a la fuente. CVSS: 9.4.

Mitigación

Cada administrador debe actualizar su servidor de Mastodon a versiones parchadas:

<https://docs.joinmastodon.org/admin/upgrading/>

Productos afectados

Mastodon versiones anteriores 3.5.17, 4.0.x anteriores a 4.0.13, 4.1.x anteriores a 4.1.13, 7 4.2.x anteriores a 4.2.5.

Enlaces

<https://github.com/mastodon/mastodon/security/advisories/GHSA-3fjr-858r-92rw>