

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	9VSA23-00901-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	20 de septiembre de 2023
Última revisión	20 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 de una nueva vulnerabilidad crítica que afecta a GitLab.

Vulnerabilidades

CVE-2023-5009

Impacto

Vulnerabilidades de riesgo crítico

CVE-2023-5009: Vulnerabilidad que permite a un atacante realizar ejecución arbitraria de código a través de políticas programadas de escaneo de seguridad. CVSS: 9.6.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

GitLab Enterprise Edition (EE) versiones anteriores a la 16.2.7
GitLab Community Edition (CE) versiones anteriores a la 16.3.4

Enlaces

<https://about.gitlab.com/releases/2023/09/18/security-release-gitlab-16-3-4-released/>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5009>