

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 | 9VSA23-00781-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 3 de febrero de 2023 |
| Última revisión | 3 de febrero 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 una vulnerabilidad crítica que afecta a dos productos de Atlassian, y para la cual la empresa ha hecho disponible un parche.

Vulnerabilidades

CVE-2023-22501

Impacto

Vulnerabilidades de riesgo crítico

CVE-2023-22501: Vulnerabilidad de autenticación en Jira Service Management Server y Data Center permite a un atacante hacerse pasar por otro usuario y ganar acceso a una instancia de Jira Service Management bajo algunas circunstancias.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

Jira Service Management Server y Data Center 5.3.0, 5.3.1, 5.3.2, 5.4.0, 5.4.1, 5.5.0.

Enlaces

<https://confluence.atlassian.com/jira/jira-service-management-server-and-data-center-advisory-cve-2023-22501-1188786458.html>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22501>

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://www.linkedin.com/company/csirt-gob>