| | |
|---|---|
| **Alerta de seguridad cibernética** | 9VSA23-00837-01 |
| **Clase de alerta** | Vulnerabilidad |
| **Tipo de incidente** | Sistema y/o Software Abierto |
| **Nivel de riesgo** | Crítico |
| **TLP** | Blanco |
| **Fecha de lanzamiento original** | 25 de mayo de 2023 |
| **Última revisión** | 25 de mayo 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 afecta a actualizaciones.

## Resumen


El CSIRT de Gobierno comparte información de una nueva vulnerabilidad crítica que afecta a GitLab Community Edition (CE) y Enterprise Edition (EE), y para la cual ya fue liberado un parche, parte de la versión 16.0.1 de la plataforma.


## Vulnerabilidades

CVE-2023-2825

## Impacto

### Vulnerabilidades críticas

CVE-2023-2825: Un usuario malicioso no autenticado puede usar esta vulnerabilidad de salto de directorios (path traversal) para leer archivos arbitrarios en el servidor, cuando un adjunto existe en un proyecto público anidado en al menos cinco grupos.

### Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

### Productos afectados

GitLab Community Edition (CE) y Enterprise Edition (EE) desde la versión 16.0.0.

### Enlaces

https://about.gitlab.com/releases/2023/05/23/critical-security-release-gitlab-16-0-1-released/

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-2825

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.05.25 09:52:12 -04'00'