Alerta de seguridad cibernética	9VSA24-00962-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	23 de enero de 2024
Última revisión	23 de enero 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 parchada por GitLab en su versión 16.1.0 de GitLab Community Edition (CE) y Enterprise Edition (EE).

Vulnerabilidades

CVE-2023-7028

Impacto

Vulnerabilidades de riesgo crítico:

CVE-2023-7028: Vulnerabilidad en GitLab Community Edition (CE) y Enterprise Edition (EE), a través de la cual los emails de reseteo de las contraseñas de los usuarios podrían ser enviados a direcciones de correo electrónico no verificadas. CVSS: 10.

Mitigación

Actualizar GitLab a sus versiones 16.7.3, 16.6.5 o 16.5.7 (https://about.gitlab.com/releases/2024/01/12/gitlab-16-7-3-released/) y activar el segundo factor de autenticación para todas las cuentas.

Productos afectados

GitLab Community Edition (CE) y Enterprise Edition (EE) versiones 16.1 a 16.7.1.

Enlaces

https://about.gitlab.com/releases/2024/01/11/critical-security-release-gitlab-16-7-2-released/

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.01.23 11:42:13 -03'00'