Alerta de seguridad informática	9VSA20-00142-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de febrero de 2020
Última revisión	14 de febrero de 2020

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 equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de GitLab, referente a una vulnerabilidad que afecta a su característica para compartir grupos, la cual, de ser explotada, permitiría a un atacante remoto acceder a proyectos de terceros sin autorización. Este informe incluye la respectiva mitigación.

Vulnerabilidades

CVE-2020-8795

Impactos

Debido a un error en la forma de gestionar la característica de compartir grupos, es posible que al utilizar la característica se le de acceso a proyectos a usuarios no autorizados, permitiendo a un atacante visualizar proyectos ajenos.

Productos Afectados

GitLab Community Edition desde la versión 12.5.0 hasta la versión 12.7.5.

Mitigación

Dependiendo de la versión, se debe actualizar a:
Para la versión 12.7.x, actualizar a la 12.7.6.
Para la versión 12.6.x, actualizar a la 12.6.7.
Para la versión 12.5.x, actualizar a la 12.5.10.

Enlaces

https://about.gitlab.com/releases/2020/02/13/critical-security-release-gitlab-12-dot-7-dot-6-released/

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8795

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.02.14 15:47:29 -03'00'