Alerta de seguridad cibernética	9VSA21-00359-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de enero de 2021
Última revisión	11 de enero de 2021

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 la información entregada por GitLab sobre dos vulnerabilidades que afectan a GitLab Community Edition y GitLab Enterprise Edition.

Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

Vulnerabilidades

CVE-2021-22166
CVE-2020-26414

Impacto

Debido a un error al procesar las solicitudes de autenticación, un atacante remoto puede robar el token de acceso del usuario a la API a través de GitLab Pages, evadiendo el proceso de autenticación y ganando acceso no autorizado a la aplicación.

Asimismo, un atacante también puede provocar una denegación de servicio al enviar una solicitud HTTP con un método malformado en Prometeus.

Productos afectados

GitLab Community Edition: Versiones de la 11.5.0 a la 13.7.1.
GitLab Enterprise Edition: Versiones de la 11.5.0. a la 13.7.1.

Mitigación

Instalar las actualizaciones desde el sitio del proveedor.

Enlaces

https://about.gitlab.com/releases/2021/01/07/security-release-gitlab-13-7-2-released/

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22166

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26414