BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-32
Fecha de publicación: 11/09/2024
Tema: Vulnerabilidad crítica en GitLab
Traffic Light Protocol (TLP): White

Producto(s) afectado:

- GitLab CE/EE en implementaciones on-premise y versiones desde 8.14 hasta antes de 17.1.7, versiones 17.2 antes de 17.2.5 y versiones 17.3 antes de 17.3.2.

Descripción

GitLab ha corregido varias vulnerabilidades críticas, entre ellas la CVE-2024-6678, que afecta tanto a la GitLab Community Edition (CE) como a la Enterprise Edition (EE) en su implementación on-premise. Esta vulnerabilidad podría permitir a un atacante ejecutar trabajos de pipeline como otro usuario, comprometiendo la integridad de los proyectos en GitLab.

Con un CVSS de 9.9/10, la CVE-2024-6678 tiene el potencial de comprometer proyectos privados y desencadenar ataques de cadena de suministro, ya que los pipelines gestionan la compilación y despliegue del Código.

Solución

Se recomienda actualizar inmediatamente GitLab a las versiones 17.3.2, 17.2.5 o 17.1.7 para corregir esta vulnerabilidad. Si la actualización no es posible de inmediato, se aconseja deshabilitar las funciones "Security policies" y "Direct transfers" para mitigar el riesgo.
Para mas información visita el siguiente enlace: https://about.gitlab.com/releases/categories/releases/

Información adicional:

- https://www.bleepingcomputer.com/news/security/gitlab-warns-of-critical-pipeline-execution-vulnerability/
- https://thehackernews.com/2024/09/urgent-gitlab-patches-critical-flaw.html
- https://www.securityweek.com/gitlab-patches-critical-pipeline-execution-vulnerability

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com