BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-52
Fecha de publicación: 11/10/2024
Tema: Nueva Vulnerabilidad Crítica en GitLab
Traffic Light Protocol (TLP): White

Producto(s) afectado:

- GitLab Enterprise Edition (EE): **Versiones desde 12.5 a 17.2.9, desde 17.3 a 17.3.5 y de 17.4 a 17.4.2**

Descripción

Una nueva vulnerabilidad crítica en GitLab, identificada como CVE-2024-9164, ha sido descubierta, la cual permite a un atacante ejecutar pipelines con privilegios de otros usuarios. Esta vulnerabilidad afecta versiones de GitLab Enterprise Edition (EE). Con un puntaje de severidad de 9.6 sobre 10 en la escala CVSS, la vulnerabilidad es especialmente peligrosa por su capacidad de ser explotada de forma remota sin interacción del usuario y con bajos privilegios.

Los pipelines en GitLab son flujos de trabajo automatizados, como pruebas o despliegues. Si un atacante puede ejecutar pipelines sin control, podría desplegar código malicioso en entornos de producción o alterar pruebas críticas sin autorización, lo que llevaría a fallos en la seguridad o disponibilidad de servicios.

Adicional, hay cuatro vulnerabilidades destacadas con severidad alta:

- **CVE-2024-8970** (CVSS 8.2): Permite a un atacante desencadenar la ejecución de un pipeline como otro usuario bajo ciertas circunstancias. Es una vulnerabilidad crítica que podría comprometer la seguridad del sistema de CI/CD de GitLab.

- **CVE-2024-8977** (CVSS 8.2): Vulnerabilidad que permite realizar ataques SSRF en instancias de GitLab EE con el Product Analytics Dashboard configurado y habilitado. Esto podría permitir a los atacantes manipular solicitudes del servidor.

- CVE-2024-9631 (CVSS 7.5): Causa lentitud al visualizar las diferencias (diffs) de solicitudes de fusión (merge requests) con conflictos. Aunque no es crítica, afecta la usabilidad del sistema al ralentizar operaciones claves.

- CVE-2024-6530 (CVSS 7.3): Resulta en inyección HTML en la página OAuth al autorizar una nueva aplicación, debido a un problema de scripting entre sitios (XSS). Podría permitir a los atacantes ejecutar scripts maliciosos o manipular la página de autorización.

Estas vulnerabilidades también han sido corregidas con los últimos parches lanzados.

Solución

GitLab ha lanzado actualizaciones críticas que corrigen esta vulnerabilidad en las versiones 17.3.2, 17.2.5 y 17.1.7. Se recomienda a los usuarios aplicar inmediatamente los parches disponibles.

Una mitigación temporal sería deshabilitar la ejecución de pipelines en ramas no protegidas y limitar el acceso a los recursos críticos a usuarios de confianza hasta que se pueda aplicar el parche de seguridad recomendado. También es recomendable revisar los permisos de los usuarios y reforzar las reglas de seguridad en las configuraciones de CI/CD para evitar explotaciones durante el período de exposición.

Para más detalles y acceso a las actualizaciones, pueden consultar la documentación oficial de GitLab

Información adicional:

- New Critical GitLab Vulnerability Could Allow Arbitrary CI/CD Pipeline Execution (thehackernews.com)
- https://about.gitlab.com/releases/2024/10/09/patch-release-gitlab-17-4-2-released/
- GitLab fixed a critical flaw that could allow arbitrary CI/CD pipeline execution (securityaffairs.com)

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com