GitLab ha publicado actualizaciones de seguridad para las ediciones Community (CE) y Enterprise (EE) para corregir ocho vulnerabilidades, incluyendo un error crítico que podría permitir la ejecución de pipelines de Integración Continua y Entrega Continua (CI/CD) en ramas no autorizadas.

Identificada como CVE-2024-9164, esta vulnerabilidad tiene una puntuación CVSS de 9.6 sobre 10.

> *«Se detectó un problema en GitLab EE que afecta a todas las versiones desde la 12.5 hasta la 17.2.9, desde la 17.3 hasta la 17.3.5, y desde la 17.4 hasta la 17.4.2, lo que permite ejecutar pipelines en ramas arbitrarias»,* explicó GitLab en su comunicado.

De los siete problemas restantes, cuatro tienen una clasificación de gravedad alta, dos son de severidad media y uno es de bajo riesgo:

- CVE-2024-8970 (puntuación CVSS: 8.2), que permite a un atacante iniciar un pipeline en nombre de otro usuario en determinadas circunstancias.
- CVE-2024-8977 (puntuación CVSS: 8.2), que posibilita ataques SSRF en instancias de GitLab EE con el Panel de Análisis de Productos habilitado.
- CVE-2024-9631 (puntuación CVSS: 7.5), que causa lentitud al visualizar diferencias en solicitudes de fusión con conflictos.
- CVE-2024-6530 (puntuación CVSS: 7.3), que provoca inyección HTML en la página OAuth cuando se autoriza una nueva aplicación, debido a un problema de cross-site scripting.

Este anuncio es parte de una serie de vulnerabilidades relacionadas con pipelines que GitLab ha revelado en los últimos meses.

El mes pasado, la empresa resolvió otro fallo crítico (CVE-2024-6678, puntuación CVSS: 9.9) que podría permitir a un atacante ejecutar trabajos de pipeline como un usuario no

autorizado.

Antes de eso, también se corrigieron tres vulnerabilidades similares: CVE-2023-5009 (puntuación CVSS: 9.6), CVE-2024-5655 (puntuación CVSS: 9.6) y CVE-2024-6385 (puntuación CVSS: 9.6).

Aunque no se ha detectado explotación activa de esta vulnerabilidad, se aconseja a los usuarios actualizar sus sistemas a la última versión disponible para evitar posibles riesgos.