GitLab ha publicado actualizaciones de seguridad para corregir 14 fallos de seguridad, incluyendo una vulnerabilidad crítica que podría ser utilizada para ejecutar pipelines de integración continua y despliegue continuo (CI/CD) como cualquier usuario.

Las vulnerabilidades, que afectan a GitLab Community Edition (CE) y Enterprise Edition (EE), han sido corregidas en las versiones 17.1.1, 17.0.3 y 16.11.5.

La más grave de estas vulnerabilidades es CVE-2024-5655 (puntuación CVSS: 9.6), que podría permitir a un atacante malintencionado iniciar un pipeline como otro usuario en ciertas circunstancias.

Afecta a las siguientes versiones de CE y EE:

- 17.1 anteriores a 17.1.1
- 17.0 anteriores a 17.0.3, y
- 15.8 anteriores a 16.11.5

GitLab indicó que la solución introduce dos cambios significativos: la autenticación GraphQL utilizando CI_JOB_TOKEN está deshabilitada por defecto y los pipelines ya no se ejecutarán automáticamente cuando una solicitud de fusión sea redirigida después de que su rama de destino anterior sea fusionada.

Algunos de los otros fallos importantes corregidos en la última versión son:

- CVE-2024-4901 (puntuación CVSS: 8.7) – Una vulnerabilidad de XSS almacenada que podría ser importada desde un proyecto con notas de commits maliciosas
- CVE-2024-4994 (puntuación CVSS: 8.1) – Un ataque CSRF en la API GraphQL de GitLab que permite la ejecución de mutaciones arbitrarias de GraphQL
- CVE-2024-6323 (puntuación CVSS: 7.5) – Una falla de autorización en la función de búsqueda global que permite la filtración de información sensible de un repositorio privado dentro de un proyecto público
- CVE-2024-2177 (puntuación CVSS: 6.8) – Una vulnerabilidad de falsificación entre

ventanas que permite a un atacante abusar del flujo de autenticación OAuth mediante una carga útil manipulada

Aunque no se ha detectado explotación activa de estas vulnerabilidades, se recomienda a los usuarios aplicar los parches para mitigar posibles amenazas.