Investigadores de seguridad cibernética revelaron los detalles de una nueva vulnerabilidad de seguridad en GitLab, un software DevOps de código abierto, que podría permitir que un atacante remoto no autenticado recupere información relacionada con el usuario.

Rastreada como CVE-2021-4191, con puntaje CVSS de 5.3, la falla de la gravedad media afecta a todas las versiones de GitLab Community Edition y Enterprise Edition a partir de la 13.0 y a todas las versiones a partir de la 14.4 y anteriores a la 14.8.

Jake Baines, investigador senior de seguridad de Rapid7, obtuvo el crédito por descubrir y reportar la falla. Después de la divulgación responsable el 18 de noviembre de 2021, se lanzaron parches para servidores autoadministrados como parte de las versiones de seguridad crítica de GitLab 14.8.2, 14.7.4 y 14.6.5 enviadas el 25 de febrero de 2022.

> *«La vulnerabilidad es el resultado de una falta de verificación de autenticación al ejecutar ciertas consultas de la API de GitLab GraphQL. Un atacante remoto no autenticado puede usar esta vulnerabilidad para recopilar nombres de usuario, nombres y direcciones de correo electrónico registrados en GitLab»*, dijo Baines.

La explotación exitosa de la fuga de información de la API podría permitir a los atacantes enumerar y compilar listas de nombres de usuario legítimos que pertenecen a un objetivo que luego se puede utilizar como un trampolín para realizar ataques de fuerza bruta, incluida la adivinación de contraseñas, la difusión de contraseñas y el relleno de credenciales.

> *«La fuga de información también permite potencialmente que un atacante cree una nueva lista de palabras de nombre de usuario basada en las instalaciones de GitLab, no solo desde gitlab.com sino también desde las otras 50,000 instancias de GitLab a las que se puede acceder desde Internet»,* dijo Baines.

Además de CVE-2021-4191, el parche también aborda otras seis fallas de seguridad, una de

las cuales es un problema crítico (CVE-2022-0735, con puntaje CVSS de 9.6), que permite a un atacante desviar los tokens de registro del corredor utilizados para autenticar y autorizar trabajos de CI/CD alojados en instancias de GitLab.