La plataforma DevOps GitLab lanzó actualizaciones de software para abordar una vulnerabilidad de seguridad crítica, que de ser explotada potencialmente, podría permitir que un atacante tome el control de las cuentas.

Rastreada como CVE-2022-1162, la falla tiene un puntaje CVSS de 9.1 y se dice que fue descubierta internamente por el equipo de GitLab.

> *«Se estableció una contraseña codificada para las cuentas registradas con un proveedor de OmniAuth (p. ej., OAuth, LDAP, SAML) en GitLab CE/EE versiones 14.7 anteriores a 14.7.7, 14.8 anteriores a 14.8.5 y 14.9 anteriores a 14.9.2 que permiten a los atacantes potencialmente tomar el control de las cuentas»,* dijo la compañía.

GitLab, que solucionó el problema con la última actualización de las versiones 14.9.2, 14.8.5 y 14.7.7 para GitLab Community Edition (CE) y Enterprise Edition (EE), también dijo que tomó la medida des restablecer la contraseña de un número no especificado de usuarios por precaución.

> *«Nuestra investigación no muestra indicios de que los usuarios o las cuentas se hayan visto comprometidos»,* agregó la compañía.

Además, la empresa publicó un script que los administradores de instancias autogestionadas pueden ejecutar para identificar cuentas potencialmente afectadas por CVE-2022-1162. Una vez que se identifican las cuentas afectadas, se recomienda restablecer la contraseña.

GitLab también abordó como parte de la actualización de seguridad, dos errores de

secuencias de comandos entre sitios almacenados (XSS) de alta gravedad (CVE-2022-1175 y CVE-2022-1190), así como nueve fallas de gravedad media y cinco problemas que son calificados con gravedad baja.