GitLab se movió para abordar una vulnerabilidad de seguridad crítica en su servicio, que de ser explotada exitosamente, podría resultar en una apropiación de la cuenta.

Rastreada como CVE-2022-1680, la vulnerabilidad tiene una puntuación de gravedad CVSS de 9.9, y fue descubierta internamente por la compañía. La falla de seguridad afecta a todas las versiones de GitLab Enterprise Edition (EE) desde la 11.0 a la 14.9.5, todas las versiones desde la 14.10 hasta la 14.10.4 y todas las versiones desde la 15.0 hasta la 15.0.1.

> *«Cuando se configura el SSO SAML grupal, la función SCIM (disponible solo en suscripciones Premium+) puede permitir que cualquier propietario de un grupo Premium invite a usuarios arbitrarios a través de su nombre de usuario y correo electrónico, y luego cambie las direcciones de correo electrónico de esos usuarios por medio de SCIM a un correo electrónico controlado por un atacante y por lo tanto, en ausencia de 2FA, hacerse cargo de esas cuentas»*, dijo GitLab.

Al lograr esto, un hacker también puede cambiar el nombre para mostrar el nombre de usuario de la cuenta objetivo, según advirtió el proveedor de la plataforma DevOps en su aviso publicado el 1 de junio de 2022.

GitLab también resolvió en las versiones 15.0.1, 14.10.4 y 14.9.5 otras siete vulnerabilidades de seguridad, dos de las cuales tienen calificación alta, cuatro tienen calificación media y una tiene calificación baja en gravedad.