GitLab ha lanzado actualizaciones de seguridad para abordar dos vulnerabilidades críticas, incluida una que podría ser explotada para tomar el control de cuentas sin requerir ninguna acción por parte del usuario.

La vulnerabilidad, identificada como CVE-2023-7028, ha sido calificada con la máxima gravedad de 10.0 en el sistema de puntuación CVSS y podría facilitar la toma de control de cuentas al enviar correos electrónicos de restablecimiento de contraseña a una dirección de correo electrónico no verificada.

La plataforma DevSecOps ha señalado que esta vulnerabilidad se origina en un error dentro del proceso de verificación de correo electrónico, que permitía a los usuarios restablecer sus contraseñas a través de una dirección de correo electrónico secundaria.

Esta vulnerabilidad afecta a todas las instancias autoadministradas de GitLab Community Edition (CE) y Enterprise Edition (EE) que utilizan las siguientes versiones:

- 16.1 antes de 16.1.6
- 16.2 antes de 16.2.9
- 16.3 antes de 16.3.7
- 16.4 antes de 16.4.5
- 16.5 antes de 16.5.6
- 16.6 antes de 16.6.4
- 16.7 antes de 16.7.2

GitLab ha afirmado que ha abordado este problema en las versiones 16.5.6, 16.6.4 y 16.7.2, además de retrotraer la corrección a las versiones 16.1.6, 16.2.9, 16.3.7 y 16.4.5. La compañía también ha destacado que este fallo fue introducido en la versión 16.1.0 el 1 de mayo de 2023.

> *«En estas versiones, todas las formas de autenticación se ven afectadas. Además, los usuarios que tienen habilitada la autenticación de dos factores son vulnerables*

> *al restablecimiento de la contraseña, pero no a la toma de control de la cuenta, ya que se requiere su segundo factor de autenticación para iniciar sesión»,* ha indicado GitLab.

GitLab también ha solucionado otra vulnerabilidad crítica (CVE-2023-5356, puntuación CVSS: 9.6) como parte de la última actualización. Esta vulnerabilidad permite que un usuario abuse de las integraciones de Slack/Mattermost para ejecutar comandos de barra como otro usuario.

Para mitigar cualquier amenaza potencial, se recomienda actualizar las instancias a una versión parcheada tan pronto como sea posible y habilitar la autenticación de dos factores, en caso de que aún no esté activada, especialmente para los usuarios con privilegios elevados.