La Agencia de Ciberseguridad e Infraestructura de los Estados Unidos (CISA) ha incluido en su catálogo de Vulnerabilidades Conocidas Explotadas (KEV) una grave falla que afecta a GitLab, debido a la activa explotación que está teniendo lugar.

Identificado como CVE-2023-7028 (puntuación CVSS: 10.0), este fallo de máxima gravedad podría permitir la toma de control de cuentas al enviar correos electrónicos de restablecimiento de contraseña a una dirección de correo electrónico no verificada.

GitLab, que reveló los detalles de esta deficiencia a principios de enero, indicó que se introdujo como parte de un cambio de código en la versión 16.1.0 lanzada el 1 de mayo de 2023.

> *«Estas versiones son afectadas por todos los mecanismos de autenticación. Además, los usuarios con autenticación de dos factores están en riesgo de restablecimiento de contraseña, aunque no de toma de control de cuenta, ya que se requiere el segundo factor para iniciar sesión»,* señaló la compañía en ese momento.

La explotación exitosa de este problema puede tener consecuencias graves, permitiendo no solo la toma de control de una cuenta de usuario de GitLab, sino también el robo de información sensible, credenciales e incluso la inserción de código malicioso en repositorios de código fuente, lo que facilitaría ataques a la cadena de suministro.

> *«Por ejemplo, un atacante que obtenga acceso a la configuración del pipeline de CI/CD podría incrustar código malicioso diseñado para extraer datos sensibles, como información de identificación personal (PII) o tokens de autenticación, y redirigirlos a un servidor controlado por el atacante»,* explicó la firma de seguridad en la nube Mitiga en un informe reciente.

> *«Del mismo modo, modificar el código del repositorio podría implicar la inserción de malware que comprometa la integridad del sistema o introduzca puertas traseras para acceso no autorizado. El código malicioso o el abuso del pipeline podrían conducir al robo de datos, interrupción del código, acceso no autorizado y ataques a la cadena de suministro».*

La vulnerabilidad ha sido solucionada en las versiones 16.5.6, 16.6.4 y 16.7.2 de GitLab, con los parches también aplicados a las versiones anteriores 16.1.6, 16.2.9, 16.3.7 y 16.4.5.

CISA aún no ha proporcionado detalles adicionales sobre cómo se está explotando esta vulnerabilidad en ataques reales. Dada la explotación activa, se requiere que las agencias federales apliquen las últimas correcciones antes del 22 de mayo de 2024 para proteger sus redes.