BOLETÍN DE ALERTA

Boletín Nro.: 2024-02
Fecha de publicación: 15/01/2024
Tema: Vulnerabilidad crítica en GitLab CE/EE envío de correos de restablecimiento de contraseña a direcciones no verificadas

Productos afectados:
Versiones anteriores de GitLab Community Edition (CE) y Enterprise Edition (EE):

- 16.1 hasta 16.1.5
- 16.2 hasta 16.2.8
- 16.3 hasta 16.3.6
- 16.4 hasta 16.4.4
- 16.5 hasta 16.5.6
- 16.6 hasta 16.6.4
- 16.7 hasta 16.7.2

Descripción:

Se ha reportado una vulnerabilidad de severidad crítica, en GitLab CE/EE se ha asignado el identificador CVE-2023-7028. Que permitiría a un actor malicioso solicitar correos de restablecimiento de credenciales contraseñas de las cuentas de usuario de los administradores de GitLab y enviarlas a una cuenta de correo sin verificar.

Impacto:

Un actor malicioso podría tomar el control de las cuentas de usuario de los administradores de la plataforma a través del proceso de restablecimiento de contraseñas.

Recomendación:

Se recomienda a los administradores de instancias GitLab actualizar a la versión parcheada de inmediato (16.7.2, 16.6.4, 16.5.6) y habilitar la autenticación de dos factores (2FA) para todas las cuentas de GitLab, especialmente para las cuentas de administrador.

Información adicional:

- https://about.gitlab.com/releases/2024/01/11/critical-security-release-gitlab-16-7-2-released/
- https://nvd.nist.gov/vuln/detail/CVE-2023-7028
- https://www.helpnetsecurity.com/2024/01/12/cve-2023-7028/