BOLETÍN DE ALERTA

Boletín Nro.: 2024-08
Fecha de publicación: 31/01/2024
Tema: Actualizaciones de seguridad en GitLab

Productos afectados:

- versiones de GitLab CE/EE desde 12.7 hasta 16.8.1

Descripción:

Se han reportado varias vulnerabilidades de seguridad en GitLab CE/EE, incluyendo una de severidad crítica identificada como CVE-2024-0402 que permitiría a un usuario autenticado escribir archivos en ubicaciones arbitrarias del servidor de GitLab mientras crea un espacio de trabajo. Además, se han reportado otras cuatro vulnerabilidades de severidad media las cuales se detallan a continuación:

- CVE-2023-6159 (CVSS 6.5): Denegación de Servicio de Expresiones Regulares (ReDoS) a través de Cargo.toml que contenga una entrada maliciosa especialmente elaborada.
- CVE-2023-5933 (CVSS 6.4): La sanitización inadecuada de la entrada del nombre de usuario permite solicitudes PUT arbitrarias a través de la API.
- CVE-2023-5612 (CVSS 5.3): Vulnerabilidad que permite al actor malicioso leer la dirección de correo electrónico a través del tag del feed RSS, aun si la visibilidad en el perfil del usuario estuviera deshabilitada.
- CVE-2024-0456 (CVSS 4.3): Un atacante no autorizado puede asignar usuarios arbitrarios a solicitudes de extracción (MR) que hayan sido creadas dentro del proyecto de GitLab.

Impacto:

Estas vulnerabilidades presentan riesgos críticos o de severidad media que podrían permitir a atacantes realizar acciones no autorizadas o acceder a información sensible.

Recomendación:

Se recomienda instalar las últimas actualizaciones desde la página oficial de GitLab.

Información adicional:

- https://about.gitlab.com/releases/2024/01/25/critical-security-release-gitlab-16-8-1-released/
- https://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-en-gitlab-0
- https://nvd.nist.gov/vuln/detail/CVE-2024-0402