BOLETÍN DE ALERTA

Boletín Nro.: 2023-45
Fecha de publicación: 20/09/2023
Tema: **Alerta de Seguridad para Community Edition (CE) y Enterprise Edition (EE) de GitLab**

Productos afectados:

- GitLab Community Edition (CE) y Enterprise Edition (EE), versiones desde 13.12 y anteriores a 16.2.7.
- GitLab Community Edition (CE) y Enterprise Edition (EE), versiones desde 16.3 y anteriores a 16.3.4.

Descripción:

Se ha reportado un nuevo aviso de seguridad sobre una vulnerabilidad que afecta a GitLab Community Edition (CE) y Enterprise Edition (EE), que permitiría a un atacante realizar ejecución arbitraria de trabajos (*Jobs*) en el sistema afectado.

La vulnerabilidad identificada como CVE-2023-4998, de severidad "Crítica" y sin puntuación asignada aún. Se debe a una falla de seguridad en GitLab Community Edition (CE) y Enterprise Edition (EE). Que permitiría a un actor malicioso ejecutar pipelines (procesos automatizados) como si fuera otro usuario, aprovechando las políticas de ejecución de escaneos de seguridad programados en los producos afectados.

Impacto:

La explotación exitosa de esta vulnerabilidad podría permitir a un actor malicioso realizar ejecución arbitraria de trabajos (*Jobs*) en el sistema afectado.

Solución:

Recomendamos instalar las actualizaciones correspondientes provistas por el fabricante a través de la siguiente guía:

- https://about.gitlab.com/update/

Información adicional:

- https://www.incibe.es/incibe-cert/alerta-temprana/avisos/vulnerabilidad-en-community-edition-ce-y-enterprise-edition-ee-0
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4998
- https://about.gitlab.com/releases/2023/09/18/security-release-gitlab-16-3-4-released/
- https://about.gitlab.com/update/