



## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilités dans les produits Gitlab
<b>Numéro de Référence</b>	46802903/24
<b>Date de Publication</b>	29 Mars 2024
<b>Risque</b>	Important
<b>Impact</b>	Important

### Systemes affectés

- GitLab Community Edition (CE) et Enterprise Edition (EE) versions 16.10.x antérieures à 16.10.1
- GitLab Community Edition (CE) et Enterprise Edition (EE) versions 16.9.x antérieures à 16.9.3
- GitLab Community Edition (CE) et Enterprise Edition (EE) versions antérieures à 16.8.5

### Identificateurs externes

- CVE-2023-6371
- CVE-2024-2818

### Bilan de la vulnérabilité

Gitlab annonce la correction de deux vulnérabilités dans les produits susmentionnés. L'exploitation réussie de ces vulnérabilités pourrait permettre à un attaquant de causer un déni de service et d'injecter de code indirect à distance (XSS).

### Solution

Veillez se référer au bulletin de sécurité Gitlab du 27 mars 2024 pour plus d'information.

### Risque

- Déni de service
- Injection de code indirecte à distance (XSS)

### Annexe

Bulletin de sécurité Gitlab du 27 mars 2024:

- <https://about.gitlab.com/releases/2024/03/27/security-release-gitlab-16-10-1-released/>