



.....
Centre de Veille de Détection et de
Réaction aux Attaques Informatiques

BULLETIN DE SECURITE

Titre	Vulnérabilités corrigées dans GitLab
Numéro de Référence	40371602/23
Date de publication	16 Février 2023
Risque	Important
Impact	critique

Systemes affectés

- GitLab Community Edition (CE) et Enterprise Edition (EE) versions antérieures à 15.6.8
- GitLab Community Edition (CE) and Enterprise Edition (EE) versions 15.7.x antérieures à 15.7.7
- GitLab Community Edition (CE) and Enterprise Edition (EE) versions 15.8.x antérieures à 15.8.2

Identificateurs externes

- CVE-2023-23946 CVE-2023-22490

Bilan de la vulnérabilité

GitLab annonce la disponibilité de mises à jour permettant de corriger deux vulnérabilités affectant ses produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'exécuter du code arbitraire ou d'exfiltrer des données confidentielles.

Solution

Veuillez-vous référer au bulletin de sécurité de GitLab afin d'installer les nouvelles mises à jour.

Risque

- Exécution de code arbitraire à distance
- Exfiltration de données confidentielles

Référence

Bulletin de sécurité de GitLab

- <https://about.gitlab.com/releases/2023/02/14/critical-security-release-gitlab-15-8-2-released/>