



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

BULLETIN DE SECURITE

Titre	Vulnérabilité critique affectant GitLab
Numéro de Référence	41791005/23
Date de publication	10 Mai 2023
Risque	Important
Impact	critique

Systemes affectés

- GitLab Community Edition (CE) versions 15.10 antérieures à la version 15.10.6
- GitLab Community Edition (CE) versions 15.11 antérieures à la version 15.11
- GitLab Community Edition (CE) versions 15.4.x à 15.9.x antérieures à la version 15.9.7
- GitLab Enterprise Edition (EE) versions 15.10 antérieures à la version 15.10.6
- GitLab Enterprise Edition (EE) versions 15.11 antérieures à la version 15.11
- GitLab Enterprise Edition (EE) versions 15.4.x à 15.9.x antérieures à la version 15.9.7

Identificateurs externes

- CVE-2023-2478

Bilan de la vulnérabilité

GitLab annonce la disponibilité de mises à jour permettant de corriger une vulnérabilité critique affectant ses produits susmentionnés. L'exploitation de cette vulnérabilité peut permettre à un attaquant distant d'exécuter du code arbitraire.

Solution

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

Risque

- Exécution de code arbitraire à distance

Référence

Bulletin de sécurité de GitLab

- <https://about.gitlab.com/releases/2023/05/05/critical-security-release-gitlab-15-11-2-released/>