



BULLETIN DE SECURITE

Titre	Vulnérabilité critique dans GitLab
Numéro de Référence	39821801/23
Date de Publication	18 janvier 2023
Risque	Critique
Impact	Critique

Systèmes affectés

- GitLab Community Edition (CE) et Enterprise Edition (EE) versions 15.7.x antérieures à 15.7.5
- GitLab Community Edition (CE) et Enterprise Edition (EE) versions 15.6.x antérieures à 15.6.6
- GitLab Community Edition (CE) et Enterprise Edition (EE) versions 15.5.x antérieures à 15.5.9

Identificateurs externes

- CVE-2022-41903, CVE-2022-23521

Bilan de la vulnérabilité

GitLab a publié une mise à jour de sécurité pour corriger une vulnérabilité critique dans ses éditions Community Edition (CE) et Enterprise Edition (EE). L'exploitation réussie de cette vulnérabilité pourrait permettre à un utilisateur authentifié non autorisé d'exécuter du code arbitraire sur le serveur.

Solution

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

Risque

- Exécution du code arbitraire,

Référence

Bulletin de sécurité GitLab du 17 Janvier 2023:

- <https://about.gitlab.com/releases/2023/01/17/critical-security-release-gitlab-15-7-5-released/>