



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

BULLETIN DE SECURITE

Titre	Vulnérabilité critique affectant GitLab
Numéro de Référence	42062505/23
Date de publication	10 Mai 2023
Risque	Critique
Impact	Critique

Systemes affectés

- GitLab Community Edition (CE) et Enterprise Edition (EE) versions 16.0.x antérieures à 16.0.1

Identificateurs externes

- CVE-2023-2825

Bilan de la vulnérabilité

GitLab annonce la disponibilité de mises à jour permettant de corriger une vulnérabilité très critique affectant ses produits susmentionnés. L'exploitation de cette vulnérabilité peut permettre à un attaquant distant d'accéder à des informations confidentielles.

Solution

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

Risque

- Accès à des informations confidentielles

Référence

Bulletin de sécurité de GitLab

- <https://about.gitlab.com/releases/2023/05/23/critical-security-release-gitlab-16-0-1-released/>