



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

BULLETIN DE SECURITE

Titre	Vulnérabilités affectant GitLab
Numéro de Référence	56751109/25
Date de publication	11 Septembre 2025
Risque	Important
Impact	Important

Systemes affectés

- GitLab Community Edition (CE) et Enterprise Edition (EE) versions antérieures à 18.3.2, 18.1.6 et 18.2.6

Identificateurs externes

CVE-2025-10094 CVE-2025-1250 CVE-2025-2256 CVE-2025-6454 CVE-2025-6769
CVE-2025-7337

Bilan de la vulnérabilité

GitLab annonce la disponibilité de mises à jour permettant de corriger plusieurs vulnérabilités affectant ses produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'accéder à des données confidentielles, de falsifier des requêtes côté serveur ou de causer un déni de service.

Solution

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

Risque

- Accès à des données confidentielles
- Falsification de requêtes coté serveur
- Déni de service

Référence

Bulletin de sécurité de GitLab :

- <https://about.gitlab.com/releases/2025/09/10/patch-release-gitlab-18-3-2-released/>