



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

BULLETIN DE SECURITE

Titre	Vulnérabilités affectant GitLab
Numéro de Référence	57082609/25
Date de publication	26 septembre 2025
Risque	Important
Impact	Important

Systemes affectés

- GitLab Community Edition (CE) et Enterprise Edition (EE) versions antérieures à 18.3.3, 18.4.1 et 18.2.7

Identificateurs externes

CVE-2025-10858 CVE-2025-10867 CVE-2025-10868 CVE-2025-10871 CVE-2025-5069
CVE-2025-7691 CVE-2025-8014 CVE-2025-8713 CVE-2025-8714 CVE-2025-8715
CVE-2025-9958

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, d'élever des privilèges ou de causer un déni de service.

Solution

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

Risque

- Accès à des données confidentielles
- Elévation de privilèges
- Dénî de service

Référence

Bulletin de sécurité de GitLab :

- <https://about.gitlab.com/releases/2025/09/25/patch-release-gitlab-18-4-1-released/>