



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

BULLETIN DE SECURITE

| | |
|----------------------------|---------------------------------|
| Titre | Vulnérabilités affectant GitLab |
| Numéro de Référence | 59820801/26 |
| Date de publication | 08 Janvier 2026 |
| Risque | Important |
| Impact | Important |

Systemes affectés

- GitLab Community Edition (CE) et Enterprise Edition (EE) versions antérieures à 18.7.1, 18.6.3 et 18.5.5

Identificateurs externes

CVE-2025-3950 CVE-2025-9222 CVE-2025-10569 CVE-2025-11246 CVE-2025-13761
CVE-2025-13772 CVE-2025-13781

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 d'exécuter du code arbitraire à distance, contourner des mesures de sécurité, d'accéder à des données confidentielles 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

- Exécution de code arbitraire à distance
- Contournement de mesures de sécurité
- Accès à des données confidentielles
- Dénier de service

Référence

Bulletin de sécurité de GitLab :

- <https://about.gitlab.com/releases/2026/01/07/patch-release-gitlab-18-7-1-released/>