



BULLETIN DE SECURITE

Titre	Vulnérabilités dans GitLab
Numéro de Référence	61452502/26
Date de Publication	25 Février 2026
Risque	Important
Impact	Important

Systèmes affectés

- GitLab Community Edition (CE) et Gitlab Enterprise Edition (EE) versions 18.8.x antérieures à 18.8.5
- GitLab Community Edition (CE) et Gitlab Enterprise Edition (EE) versions 18.9.x antérieures à 18.9.1
- GitLab Community Edition (CE) et Gitlab Enterprise Edition (EE) versions antérieures à 18.7.5

Identificateurs externes

- CVE-2025-14103 CVE-2025-14511 CVE-2025-3525 CVE-2026-0752
- CVE-2026-1388 CVE-2026-1662 CVE-2026-1725 CVE-2026-1747
- CVE-2026-2845

Bilan de la vulnérabilité

GitLab a publié une mise à jour de sécurité pour corriger plusieurs vulnérabilités dans ses éditions Community Edition (CE) et Enterprise Edition (EE). L'exploitation réussie de ces vulnérabilités pourrait permettre à un attaquant de contourner la politique de sécurité, de provoquer un déni de service à distance, d'injecter de code indirecte à distance (XSS) et de porter atteinte à la confidentialité des données.

Solution

Veuillez se référer au bulletin de sécurité GitLab du 25 Février 2026, afin d'installer les nouvelles mises à jour.

Risque

- Contournement de la politique de sécurité ;
- Atteinte à la confidentialité des données ;

- Injection de code indirecte à distance (XSS) ;
- Déni de service à distance ;

Référence

Bulletin de sécurité GitLab du 25 Février 2026:

- <https://about.gitlab.com/releases/2026/02/25/patch-release-gitlab-18-9-1-released/>