AVIS DE SECURITE

Objet	**Multiples vulnérabilités dont une critique dans GitLab CE/EE (CVE-2026-110264)**
Niveau de criticité	**CRITIQUE**
Référence	SNCSIRT-2026-ADS-279
TLP	WHITE

Résumé

GitLab a publié le 21 octobre 2026 les versions correctives 19.5.1, 19.4.3 et 19.3.6 (ainsi que 19.2.9, 19.1.9, 19.0.10 et 18.11.13). Douze vulnérabilités sont corrigées, dont CVE-2026-110264, un dépassement d'entier dans le compilateur d'expressions régulières noté CVSS 10.0, ainsi que CVE-2026-15723 (authentification incorrecte, 8.2) et CVE-2026-112212 (empoisonnement de cache OAuth/OIDC, 7.5).

Risque de sécurité

- Exécution de code arbitraire à distance
- Atteinte à la confidentialité des données
- Contournement de la politique de sécurité
- Déni de service

Systèmes affectés

- GitLab CE/EE versions antérieures à 19.3.6
- GitLab CE/EE 19.4.x antérieures à 19.4.3
- GitLab CE/EE 19.5.x antérieures à 19.5.1

Recommandations

Se référer au bulletin de sécurité de l'éditeur du 21/10/2026 :

- https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-5-1-released/