



DJ-CERT

Centre national de veille,
d'alerte et de réponse aux
attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 22-10-2026

BULLETIN ALERTES

Object	Vulnérabilité dans Gitlab CE/EE(CVE-2026-110264)
Référence	1508
Date de Publication	2026-10-21
Sévérité	Critique

IMPACT :

- Exécution de code arbitraire à distance, sans authentification

SYSTÈME AFFECTÉ :

- GitLab CE/EE (installations auto-hébergées) versions 7.0 à 18.11 antérieures à 18.11.13
- GitLab CE/EE versions 19.0 antérieures à 19.0.10
- GitLab CE/EE versions 19.1 antérieures à 19.1.9
- GitLab CE/EE versions 19.2 antérieures à 19.2.9
- GitLab CE/EE versions 19.3 antérieures à 19.3.6
- GitLab CE/EE versions 19.4 antérieures à 19.4.3
- GitLab CE/EE versions 19.5 antérieures à 19.5.1

DÉSCRIPTION :

Une vulnérabilité critique a été corrigée dans GitLab Community Edition et Enterprise Edition. Elle résulte d'un dépassement d'entier lors de la compilation d'expressions régulières. L'exploitation de cette faille permet à un attaquant non authentifié d'exécuter du code arbitraire sur le serveur GitLab.



SOLUTION :

Mettre à jour GitLab vers l'une des versions corrigées suivantes :

- 19.5.1 ou une version ultérieure
- 19.4.3 ou une version ultérieure
- 19.3.6 ou une version ultérieure
- 19.2.9 ou une version ultérieure
- 19.1.9 ou une version ultérieure
- 19.0.10 ou une version ultérieure
- 18.11.13 ou une version ultérieure

CONTOURNEMENT PROVISoire :

Aucun contournement n'est disponible.

DOCUMENTATION :

Bulletin de sécurité GitLab :

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

CVE-2026-110264 :

- <https://www.cve.org/CVERecord?id=CVE-2026-110264>