DJ-CERT | Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 13-09-2026

BULLETIN ALERTES

Object	Vulnérabilité affectant GitLab
Réference	1499
Date de Publication	2026-09-13
Sévérité	Critique

IMPACT :

- Lecture de fichiers arbitraires sur le serveur
- Divulgation d'informations sensibles

SYSTÉME AFFECTÉ :

- GitLab Community Edition (CE) versions 18.7 à antérieures à 19.1.8
- GitLab Enterprise Edition (EE) versions 18.7 à antérieures à 19.1.8
- GitLab CE/EE versions 19.2 antérieures à 19.2.6
- GitLab CE/EE versions 19.3 antérieures à 19.3.2

DÉSCRIPTION :

Une vulnérabilité critique a été corrigée dans GitLab Community Edition et Enterprise Edition. Elle résulte d'un défaut de confinement des chemins d'accès combiné à une absence de contrôle d'authentification au niveau de l'API des commits de dépôt. Son exploitation permet à un attaquant non authentifié de lire des fichiers arbitraires sur le serveur GitLab, exposant potentiellement des informations sensibles ou fichiers de configuration.

SOLUTION :

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

- 19.1.8 ou une version ultérieure
- 19.2.6 ou une version ultérieure
- 19.3.2 ou une version ultérieure

DOCUMENTATION :

Bulletin de sécurité GitLab :

- https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-3-2-released/

CVE-2026-85706 :

- https://www.cve.org/CVERecord?id=CVE-2026-85706