



DJ-CERT

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

Autorité Nationale de Cybersécurité

Djibouti le, 22-08-2024

BULLETIN ALERTES

Objet	Multiples vulnérabilités dans GitLab
Référence	1223
Date de Publication	2024-08-22
Sévérité	Moyen

IMPACT :

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

SYSTÈME AFFECTÉ :

- GitLab Community Edition (CE) et Enterprise Edition (EE) versions 17.2.x antérieures à 17.2.4
- GitLab Community Edition (CE) et Enterprise Edition (EE) versions 17.3.x antérieures à 17.3.1
- GitLab Community Edition (CE) et Enterprise Edition (EE) versions antérieures à 17.1.6

DÉSCRIPTION :

Des vulnérabilités ont été découvertes dans GitLab. L'exploitation de ces failles pourrait permettre à un attaquant distant de provoquer une atteinte à la confidentialité des données et une atteinte à l'intégrité des données.

SOLUTION :

Mettre à jour Gitlab.(se référer à la documentation)

DOCUMENTATION :

- Bulletin de sécurité GitLab du 21 août 2024

<https://about.gitlab.com/releases/2024/08/21/patch-release-gitlab-17-3-1-released/>

- CVE-2024-3127

<https://www.cve.org/CVERecord?id=CVE-2024-3127>

- CVE-2024-6502

<https://www.cve.org/CVERecord?id=CVE-2024-6502>

- CVE-2024-7110

<https://www.cve.org/CVERecord?id=CVE-2024-7110>