



DJ-CERT

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

Autorité Nationale de Cybersécurité

Djibouti le, 19-01-2023

BULLETIN ALERTES

Objet	Une Vulnérabilité dans Gitlab
Référence	1019
Date de Publication	2023-01-19
Sévérité	Critique

IMPACT :

- Exécution de code arbitraire à distance
- Perte de confidentialité
- Perte d'intégrité

SYSTÈME AFFECTÉ :

- GitLab Community Edition (CE) et Enterprise Edition (EE) versions 15.7.x antérieures à 15.7.5
- GitLab Community Edition (CE) et Enterprise Edition (EE) versions 15.6.x antérieures à 15.6.6
- GitLab Community Edition (CE) et Enterprise Edition (EE) versions 15.5.x antérieures à 15.5.9

DÉSCRIPTION :

Une vulnérabilité a été découverte dans les produits Gitlab susmentionné .Elle permet à un attaquant distant d'exécuter du code arbitraire à distance, un contournement de la politique de sécurité et une atteinte à l'intégrité des données.

SOLUTION :

Mettre à jour vos produits Gitlab.(se réfère à la documentation)

DOCUMENTATION :

- Bulletin de sécurité GitLab du 17-01-2023
<https://about.gitlab.com/releases/2023/01/17/critical-security-release-gitlab-15-7-5-released/>
- CVE-2022-41903
<https://www.cve.org/CVERecord?id=CVE-2022-41903>
- CVE-2022-23521
<https://www.cve.org/CVERecord?id=CVE-2022-23521>