



DJ-CERT

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

Autorité Nationale de Cybersécurité

Djibouti le, 22-05-2024

BULLETIN ALERTES

| | |
|---------------------|--|
| Objet | Multiples vulnérabilités dans les Gitlab |
| Référence | 1144 |
| Date de Publication | 2024-05-22 |
| Sévérité | Critique |

IMPACT :

Atteinte à la confidentialité des données

Contournement de la politique de sécurité

Déni de service à distance

Injection de code indirecte à distance (XSS)

Injection de requêtes illégitimes par rebond (CSRF)

SYSTÈME AFFECTÉ :

GitLab Community Edition (CE) et Enterprise Edition (EE) versions 16.11.x
antérieures à 16.11.3

GitLab Community Edition (CE) et Enterprise Edition (EE) versions 17.0.x
antérieures à 17.0.1

GitLab Community Edition (CE) et Enterprise Edition (EE) versions antérieures à
16.10.6

DÉSCRIPTION :

De multiples vulnérabilités ont été découvertes dans GitLab. Certaines de ces vulnérabilités permettent à un attaquant de provoquer un déni de service à distance, de porter atteinte à la confidentialité des données et d'effectuer une injection de code indirecte à distance (XSS).

SOLUTION :

Mettre à jour GitLab:

<https://about.gitlab.com/releases/2024/05/22/patch-release-gitlab-17-0-1-released/>

DOCUMENTATION :

- CVE-2023-6502:

<https://www.cve.org/CVERecord?id=CVE-2023-6502>

- CVE-2023-7045:

<https://www.cve.org/CVERecord?id=CVE-2023-7045>

- CVE-2024-1947:

<https://www.cve.org/CVERecord?id=CVE-2024-1947>

- CVE-2024-2874:

<https://www.cve.org/CVERecord?id=CVE-2024-2874>

- CVE-2024-4367:

<https://www.cve.org/CVERecord?id=CVE-2024-4367>

- CVE-2024-4835:

<https://www.cve.org/CVERecord?id=CVE-2024-4835>