

Agence Nationale
des Systèmes d'information
de l'état

Djibouti le, 03-12-2024

BULLETIN ALERTES

Object	Multiples vulnérabilités dans GitLab
Référence	1284
Date de Publication	2024-12-03
Sévérité	Elevé

IMPACT :

- Contournement de la politique de sécurité
- Déni de service à distance
- Élévation de privilèges

SYSTÈME AFFECTÉ :

- GitLab Community Edition (CE) et Enterprise Edition (EE) versions 17.5.x antérieures à 17.5.3
- GitLab Community Edition (CE) et Enterprise Edition (EE) versions 17.6.x antérieures à 17.6.1
- GitLab Community Edition (CE) et Enterprise Edition (EE) versions antérieures à 17.4.5

DÉSCRIPTION :

Plusieurs vulnérabilités ont été découvertes dans GitLab, permettant à un attaquant de réaliser une élévation de privilèges, de provoquer un déni de service à distance et de contourner la politique de sécurité.

SOLUTION :

Consultez le bulletin de sécurité de l'éditeur pour obtenir les correctifs nécessaires (voir section Documentation).

DOCUMENTATION :

- Bulletin de sécurité GitLab du 26 novembre 2024

<https://about.gitlab.com/releases/2024/11/26/patch-release-gitlab-17-6-1-released/>

- Référence CVE CVE-2024-11668

<https://www.cve.org/CVERecord?id=CVE-2024-11668>

- Référence CVE CVE-2024-11669

<https://www.cve.org/CVERecord?id=CVE-2024-11669>

- Référence CVE CVE-2024-11828

<https://www.cve.org/CVERecord?id=CVE-2024-11828>

- Référence CVE CVE-2024-8114

<https://www.cve.org/CVERecord?id=CVE-2024-8114>

- Référence CVE CVE-2024-8177

<https://www.cve.org/CVERecord?id=CVE-2024-8177>

- Référence CVE CVE-2024-8237

<https://www.cve.org/CVERecord?id=CVE-2024-8237>