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

Autorité Nationale de Cybersécurité

Djibouti le, 16-09-2025

BULLETIN ALERTES

Object	Multiples vulnérabilités dans GitLab
Réference	1394
Date de Publication	2025-09-11
Sévérité	Elevé

IMPACT :

- Atteinte à la confidentialité des données
- Déni de service à distance
- Falsification de requêtes côté serveur (SSRF)

SYSTÉME AFFECTÉ :

- GitLab Community Edition (CE) et Gitlab Enterprise Edition (EE) versions 18.2.x antérieures à 18.2.6
- GitLab Community Edition (CE) et Gitlab Enterprise Edition (EE) versions 18.3.x antérieures à 18.3.2
- GitLab Community Edition (CE) et Gitlab Enterprise Edition (EE) versions antérieures à 18.1.6

DÉSCRIPTION :

Plusieurs vulnérabilités ont été découvertes dans GitLab. Elles peuvent être exploitées par un attaquant pour provoquer un déni de service à distance, compromettre la confidentialité des données ou réaliser une falsification de requêtes côté serveur (SSRF).

SOLUTION :

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

DOCUMENTATION :

- Bulletin de sécurité GitLab du 10 septembre 2025

https://about.gitlab.com/releases/2025/09/10/patch-release-gitlab-18-3-2-released/

- Référence CVE CVE-2025-10094

https://www.cve.org/CVERecord?id=CVE-2025-10094

- Référence CVE CVE-2025-1250

https://www.cve.org/CVERecord?id=CVE-2025-1250

- Référence CVE CVE-2025-2256

https://www.cve.org/CVERecord?id=CVE-2025-2256

- Référence CVE CVE-2025-6454

https://www.cve.org/CVERecord?id=CVE-2025-6454

- Référence CVE CVE-2025-6769

https://www.cve.org/CVERecord?id=CVE-2025-6769

- Référence CVE CVE-2025-7337

https://www.cve.org/CVERecord?id=CVE-2025-7337