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

Autorité Nationale de Cybersécurité

Djibouti le, 27-07-2025

BULLETIN ALERTES

Object	Multiples Vulnérabilités dans les produits GitLab Community Edition et Enterprise Edition
Réference	1372
Date de Publication	2025-07-25
Sévérité	Critique

IMPACT :

- Déni de service
- Injection de code indirecte à distance (XSS)
- Contournement de la politique de sécurité

SYSTÉME AFFECTÉ :

- GitLab Community Edition (CE) et Enterprise Edition (EE) versions 18.2.x antérieures à 18.2.1
- GitLab Community Edition (CE) et Enterprise Edition (EE) versions 18.1.x antérieures à 18.1.3
- GitLab Community Edition (CE) et Enterprise Edition (EE) versions 18.0.x antérieures à 18.0.5

DÉSCRIPTION :

GitLab a identifié plusieurs vulnérabilités dans les versions mentionnées de GitLab Community Edition (CE) et Enterprise Edition (EE). L'exploitation réussie de ces failles pourrait permettre à un attaquant de provoquer un déni de service, de contourner les politiques de sécurité, ainsi que d'injecter du code à distance via des vulnérabilités de type cross-site scripting (XSS).

SOLUTION :

Mettre à jour GitLab Community Edition (CE) et Enterprise Edition (EE). (se référer à la documentation)

DOCUMENTATION :

- Bulletin de sécurité Gitlab du 23 Juillet 2025:

https://about.gitlab.com/releases/2025/07/23/patch-release-gitlab-18-2-1-released/

- CVE-2025-0765:

https://nvd.nist.gov/vuln/detail/CVE-2025-0765

- CVE-2025-1299:

https://nvd.nist.gov/vuln/detail/CVE-2025-1299

- CVE-2025-4439:

https://nvd.nist.gov/vuln/detail/CVE-2025-4439

- CVE-2025-4700:

https://nvd.nist.gov/vuln/detail/CVE-2025-4700

- CVE-2025-4976:

https://www.cvedetails.com/cve/CVE-2025-4976/

- CVE-2025-7001:

https://nvd.nist.gov/vuln/detail/CVE-2025-7001