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

Autorité Nationale de Cybersécurité

Djibouti le, 16-01-2024

BULLETIN ALERTES

Object	Vulnérabilité dans le Gitlab
Réference	1092
Date de Publication	2024-01-14
Sévérité	Critique

IMPACT :

- Exécution de code arbitraire à distance
- Perte de confidentialité
- Perte d'intégrité
- Contournement de la politique de sécurité
- Elévation de privilèges

SYSTÉME AFFECTÉ :

- Gitlab Community Edition (CE) et Enterprise Edition (EE) versions 16.1.x antérieures à 16.1.6
- Gitlab Community Edition (CE) et Enterprise Edition (EE) versions 16.2.x antérieures à 16.2.9
- Gitlab Community Edition (CE) et Enterprise Edition (EE) versions 16.3.x antérieures à 16.3.7
- Gitlab Community Edition (CE) et Enterprise Edition (EE) versions 16.4.x antérieures à 16.4.5
- Gitlab Community Edition (CE) et Enterprise Edition (EE) versions 16.5.x antérieures à 16.5.6
- Gitlab Community Edition (CE) et Enterprise Edition (EE) versions 16.6.x antérieures à 16.6.4
- Gitlab Community Edition (CE) et Enterprise Edition (EE) versions 16.7.x antérieures à 16.7.2

DÉSCRIPTION :

GitLab a récemment diffusé des mises à jour de sécurité visant à remédier des vulnérabilités critiques affectons les éditions Community Edition (CE) et Enterprise Edition (EE).

La plus critique est la vulnérabilité CVE-2023-7028. , évaluée avec un score de 10 sur 10 selon le système de notation CVSSv3.

En cas d'exploitation réussie, cette faille permettrait à des attaquants d'initier des demandes de réinitialisation de mot de passe à destination d'adresses électroniques arbitraires et non vérifiées, potentiellement entraînant la compromission des comptes utilisateur. La gravité de cette menace est accentuée en l'absence d'activation de l'authentification multifactorielle.

Les utilisateurs de GitLab sont vivement encouragés à appliquer ces mises à jour de sécurité sans délai afin de prévenir tout risque de compromission de la sécurité des données.

SOLUTION :

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

DOCUMENTATION :

- Bulletin de sécurité GitLab du 11-01-2024
  https://about.gitlab.com/releases/2024/01/11/critical-security-release-gitlab-16-7-2-released/
- CVE-2023-7028
  https://www.cve.org/CVERecord?id=CVE-2023-7028