ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Vulnérabilités critiques dans les produits GitLab
Numéro de Référence	45581501/24
Date de Publication	17 Janvier 2024
Risque	Critique
Impact	Critique

Systèmes affectés

- Gitlab Community Edition (CE) et Enterprise Edition (EE) versions 16.7.x antérieures à 16.7.2
- 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 16.5.x antérieures à 16.5.6
- 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 16.3.x antérieures à 16.3.7
- 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 16.1.x antérieures à 16.1.6

Identificateurs externes

- CVE-2023-2030 CVE-2023-4812 CVE-2023-5356 CVE-2023-6955 CVE-2023-7028

Bilan de la vulnérabilité

GitLab a publié des mises à jour de sécurité pour corriger des vulnérabilités critiques (CVE-2023-7028 et CVE-2023-5356) dans ses éditions Community Edition (CE) et Enterprise Edition (EE). CVE-2023-7028 a un score CVSSv3 (Common Vulnerability Scoring System) de 10 sur 10.

Les vulnérabilités critiques sont les suivantes :

CVE-2023-7028 : L'exploitation réussie de cette vulnérabilité pourrait permettre à des attaquants d'envoyer des demandes de réinitialisation de mot de passe à des adresses électro-

niques arbitraires et non vérifiées, permettant ainsi la prise de contrôle du compte, en particulier si l'authentification multifactorielle n'est pas activée.

CVE-2023-5356 : Une exploitation réussie de cette vulnérabilité pourrait permettre à un attaquant d'exécuter des commandes arbitraires.

Solution

Veuillez se référer au bulletin de sécurité GitLab du 12 janvier 2024 pour plus d'information.

Risque

- Exécution de code arbitraire à distance
- Elévation de privilèges
- Contournement de la politique de sécurité
- Atteinte à la confidentialité de données

Annexe

Bulletin de sécurité GitLab du 12 janvier 2024:

- https://about.gitlab.com/releases/2024/01/11/critical-security-release-gitlab-16-7-2-released/