ROYAUME DU MAROC

ADMINISTRATION
DE LA DEFENSE NATIONALE

Direction Générale de la Sécurité des Systèmes d'Information

Centre de Veille de Détection et de Réaction aux Attaques Informatiques

المملكة المغربية

إدارة الدفاع الوطني

المديرية العامة لأمن نظم المعلومات

مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

BULLETIN DE SECURITE

Titre	Vulnérabilité critique affectant GitLab
Numéro de Référence	48401707/24
Date de publication	17 Juillet 2023
Risque	Critique
Impact	Critique

Systèmes affectés

- GitLab Community Edition (CE) et Enterprise Edition (EE) versions antérieures à 17.1.2, 17.0.4 et 16.11.6

Identificateurs externes

- CVE-2024-6385 CVE-2024-5257 CVE-2024-2880 CVE-2024-5470 CVE-2024-5528 CVE-2024-6595

Bilan de la vulnérabilité

GitLab annonce la disponibilité de mises à jour permettant de corriger plusieurs vulnérabilités affectant ses produits susmentionnés. Une de ces vulnérabilités identifiée par « CVE-2024-6385 » est critique. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'accéder à des informations confidentielles ou de contourner les mesures de sécurité.

Solution

Veuillez se référer au bulletin de sécurité de GitLab afin d'installer les nouvelles mises à jour.

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques
Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

Risque

- Accès à des informations confidentielles
- Contournement de mesures de sécurité

Référence

Bulletin de sécurité de GitLab

- https://about.gitlab.com/releases/2024/07/10/patch-release-gitlab-17-1-2-released/#an-attacker-can-run-pipeline-jobs-as-an-arbitrary-user