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	Vulnérabilités critiques affectant des produits Jenkins
Numéro de Référence	45802601/24
Date de publication	26 Janvier 2023
Risque	Critique
Impact	Critique

Systèmes affectés

- Jenkins weekly versions antérieures à 2.442
- Jenkins LTS versions antérieures à 2.426.3
- Git server Plugin versions antérieures à 99.101.v720e86326c09
- GitLab Branch Source Plugin versions antérieures à 688.v5fa_356ee8520
- Matrix Project Plugin versions antérieures à 822.824.v14451b_c0fd42
- Qualys Policy Compliance Scanning Connector Plugin versions antérieures à 1.0.6
- Red Hat Dependency Analytics Plugin versions antérieures à 0.9.0

Identificateurs externes

CVE-2023-6147 CVE-2023-6148 CVE-2024-23897 CVE-2024-23898 CVE-2024-23899 CVE-2024-23900 CVE-2024-23901 CVE-2024-23902 CVE-2024-23903 CVE-2024-23904 CVE-2024-23905

Bilan de la vulnérabilité

Jenkins annonce la correction de plusieurs vulnérabilités affectant ses produits susmentionnés. Une de ces vulnérabilités, identifiée par «CVE-2024-23897 » est critique et pourrait être activement exploitée. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'injecter du code dans une page, d'accéder à des informations confidentielles ou de contourner des mesures de sécurité.

Solution

Veuillez se référer au bulletin de sécurité de Jenkis pour mettre à jour votre produit.

Risques

- Accès à des informations confidentielles
- Contournement de mesures de sécurité
- Injection de contenu dans une page

Références

Bulletin de sécurité de Jenkins :

- https://www.jenkins.io/security/advisory/2024-01-24/