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 Jenkins
Numéro de Référence	41351304/23
Date de Publication	13 Avril 2023
Risque	Critique
Impact	Critique

Systèmes affectés

- Jenkins Assembla merge request builder Plugin jusqu'à la version 1.1.13
- Jenkins Azure Key Vault Plugin jusqu'à la version 187.va_cd5fecd198a_
- Jenkins Consul KV Builder Plugin jusqu'à la version 2.0.13
- Jenkins Fogbugz Plugin jusqu'à la version 2.2.17
- Jenkins Image Tag Parameter Plugin jusqu'à la version 2.0
- Jenkins Kubernetes Plugin jusqu'à la version 3909.v1f2c633e8590
- Jenkins Lucene-Search Plugin jusqu'à la version 387.v938a_ecb_f7fe9
- Jenkins NeuVector Vulnerability Scanner Plugin jusqu'à la version 1.22
- Jenkins Quay.io trigger Plugin jusqu'à la version 0.1
- Jenkins Report Portal Plugin jusqu'à la version 0.5
- Jenkins Thycotic DevOps Secrets Vault Plugin jusqu'à la version 1.0.0
- Jenkins Thycotic Secret Server Plugin jusqu'à la version 1.0.2
- Jenkins TurboScript Plugin jusqu'à la version 1.3
- Jenkins WSO2 Oauth Plugin jusqu'à la version 1.0

Identificateurs externes

- CVE-2023-28671, CVE-2023-28672, CVE-2023-28673, CVE-2023-28674, CVE-2023-28675, CVE-2023-28676, CVE-2023-28677, CVE-2023-28678, CVE-2023-28679, CVE-2023-28680, CVE-2023-28681, CVE-2023-28682, CVE-2023-28683, CVE-2023-28684, CVE-2023-28685, CVE-2023-30513 , CVE-2023-30514 , CVE-2023-30515 , CVE-2023-30516 , CVE-2023-30517 , CVE-2023-30518 , CVE-2023-30519 , CVE-2023-30520 , CVE-2023-30521 , CVE-2023-30522 , CVE-2023-30523 , CVE-2023-

30524 , CVE-2023-30525 , CVE-2023-30526 , CVE-2023-30527 , CVE-2023-30528 , CVE-2023-30529 , CVE-2023-30530 , CVE-2023-30531 , CVE-2023-30532

Bilan de la vulnérabilité

Jenkins annonce la correction de plusieurs vulnérabilités critiques affectant les produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'injecter du code dans une page, d'accéder à des informations confidentielles, d'élever ses privilèges ou de contourner la politique de sécurité.

Solution

Veuillez se référer au bulletin de sécurité Jenkins**.**

Risque

- Accès aux informations confidentielles
- Contournement de la politique de sécurité
- Injection de contenu dans une page
- Elévation de privilèges

Annexe

Bulletin de sécurité Jenkins**:**

- https://www.jenkins.io/security/advisory/2023-04-12/
- https://www.jenkins.io/security/advisory/2023-03-21/