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 affectant Zoho ManageEngine Desktop Central
Numéro de Référence	39811701/23
Date de publication	17 Janvier 2023
Risque	Important
Impact	Critique

Systèmes affectés

Si SAML-based SSO est actuellement activé :

- Vulnerability Manager Plus antérieures à 10.1.2220.18
- Browser Security Plus antérieures à 11.1.2238.6
- Device Control Plus 10.1.2220.18
- Endpoint Central antérieures à 10.1.2228.11
- Endpoint Central MSP antérieures à 10.1.2228.11
- Endpoint DLP antérieures à 10.1.2137.6
- Key Manager Plus antérieures à 6401
- OS Deployer antérieures à 1.1.2243.1
- PAM 360 antérieures à 5713
- Password Manager Pro antérieures à 12124
- Patch Manager Plus antérieures à 10.1.2220.18
- Remote Access Plus antérieures à 10.1.2228.11
- Remote Monitoring and Management (RMM) antérieures à 10.1.41
- Analytics Plus antérieures à 5150
- Application Control Plus antérieures à 10.1.2220.18
- Access Manager Plus antérieures à 4308

Si SAML-based SSO a été activé dans le passé :

- Active Directory 360 antérieures à 4310
- ADAudit Plus antérieures à 7081
- ADManager Plus antérieures à 7162
- ADSelfService Plus antérieures à 6211

- Asset Explorer antérieures à 6983
- ServiceDesk Plus antérieures à 14004
- ServiceDesk Plus MSP antérieures à 13001
- SupportCenter Plus antérieures à 11026

Identificateurs externes

- CVE-2022-47966

Bilan de la vulnérabilité

Zoho annonce la correction d'une vulnérabilité critique affectant plusieurs produits de sa solution de centralisation de gestion de parc «ManageEngine Desktop Central ». Un POC « Proof Of Concept » concernant cette vulnérabilité sera mis en ligne dans les jours à venir et son exploitation peut permettre à un attaquant distant non authentifié d'exécuter du code.

Solution

Veuillez consulter les bulletins de sécurité de ManageEngine afin d'installer les mises à jours nécessaires.

Risque

- Exécution de code à distance.

Référence

Bulletin de sécurité de ManageEngine :

- https://www.manageengine.com/security/advisory/CVE/cve-2022-47966.html