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 affectant plusieurs produits de VMware
Numéro de Référence	40650703/23
Date de publication	07 Mars 2023
Risque	Important
Impact	Important

Systèmes affectés

- Tanzu Greenplum for Kubernetes versions antérieures à 2.0.0
- Isolation Segment versions 2.8.x avec Xenial Stemcells antérieures à 621.364
- Isolation Segment versions 2.9.x avec Xenial Stemcells antérieures à 621.364
- Isolation Segment versions 2.10.x avec Xenial Stemcells antérieures à 621.364
- Isolation Segment versions 2.11.x avec Xenial Stemcells antérieures à 621.364
- Isolation Segment versions 2.12.x avec Xenial Stemcells antérieures à 621.364
- Isolation Segment versions 2.13.x avec Xenial Stemcells antérieures à 621.364
- Operations Manager versions 2.10.x antérieures à 2.10.51
- VMware Tanzu Application Service for VMs versions 2.8.x avec Xenial Stemcells antérieures à 621.364
- VMware Tanzu Application Service for VMs versions 2.9.x avec Xenial Stemcells antérieures à 621.364
- VMware Tanzu Application Service for VMs versions 2.10.x avec Xenial Stemcells antérieures à 621.364
- VMware Tanzu Application Service for VMs versions 2.11.x avec Xenial Stemcells antérieures à 621.364
- VMware Tanzu Application Service for VMs versions 2.12.x avec Xenial Stemcells antérieures à 621.364
- VMware Tanzu Application Service for VMs versions 2.13.x avec Xenial Stemcells antérieures à 621.364
- Platform Automation Toolkit versions 4.4.x antérieures à 4.4.30

- Platform Automation Toolkit versions versions 5.0.x antérieures à 5.0.23
- Isolation Segment versions 2.11.x antérieures à 2.11.25
- Isolation Segment versions 2.12.x antérieures à 2.12.15
- Isolation Segment versions 2.13.x antérieures à 2.13.10
- Operations Manager versions 3.0.x antérieures à 3.0.2
- VMware Tanzu Application Service for VMs versions 2.11.x antérieures à 2.11.31
- VMware Tanzu Application Service for VMs versions 2.12.x antérieures à 2.12.20
- VMware Tanzu Application Service for VMs versions 2.13.x antérieures à 2.13.13
- VMware Tanzu Application Service for VMs versions 3.0.x antérieures à 3.0.7. Mettre à jour Jammy Stemcells à la version supérieure ou égale à 1.80

Identificateurs externes

- CVE-2022-31706 CVE-2022-31704 CVE-2022-31710 CVE-2022-31711

Bilan de la vulnérabilité

VMware annonce la correction de trois vulnérabilités affectant ses produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant de d'exécuter du code arbitraire, accéder à des données confidentielles ou de causer un déni de service.

Solution

Veuillez se référer au bulletin de sécurité de VMware pour les mises à jour.

Risques

- Exécution de code arbitraire
- Accès à des données confidentielles
- Déni de service

Références

Bulletins de sécurité de VMware:

- https://tanzu.vmware.com/security/usn-5760-2
- https://tanzu.vmware.com/security/usn-5760-1