



BULLETIN DE SECURITE

Titre	Vulnérabilités affectant VMware Tanzu
Numéro de Référence	41931705/23
Date de publication	17 Mai 2023
Risque	Important
Impact	Important

Systèmes affectés

- Isolation Segment versions 2.10.x avec Xenial Stemcells antérieures à la version 621.376
- Isolation Segment versions 2.11.x antérieures à la version 2.11.27 avec Xenial Stemcells antérieures à la version 621.376
- Isolation Segment versions 2.12.x antérieures à la version 2.12.17 avec Xenial Stemcells antérieures à la version 621.376
- Isolation Segment versions 2.13.x antérieures à la version 2.13.12 avec Xenial Stemcells antérieures à la version 621.376
- Isolation Segment versions 2.8.x avec Xenial Stemcells antérieures à la version 621.376
- Isolation Segment versions 2.9.x avec Xenial Stemcells antérieures à la version 621.376
- Isolation Segment versions 3.0.x antérieures à la version 3.0.7 avec Jammy Stemcells antérieures à la version 1.80
- Isolation Segment versions 4.0.x avec Jammy Stemcells antérieures à la version 1.80
- Operations Manager 2.10.x versions antérieures 2.10.52
- Operations Manager 3.0.x versions antérieures 3.0.4
- Platform Automation Toolkit versions 4.0.x antérieures à la version 4.0.13
- Platform Automation Toolkit versions 4.1.x antérieures à la version 4.1.13
- Platform Automation Toolkit versions 4.2.x antérieures à la version 4.2.8
- Platform Automation Toolkit versions 4.3.x antérieures à la version 4.3.5
- Platform Automation Toolkit versions 4.4.x antérieures à la version 4.4.31
- Platform Automation Toolkit versions 5.0.x antérieures à la version 5.0.24
- Tanzu Application Service for VMs versions 2.10.x avec Xenial Stemcells antérieures à la version 621.376
- Tanzu Application Service for VMs versions 2.11.x antérieures à la version 2.11.33 avec Xenial Stemcells antérieures à la version 621.376

- Tanzu Application Service for VMs versions 2.12.x antérieures à la version 2.12.22 avec Xenial Stemcells antérieures à la version 621.376
- Tanzu Application Service for VMs versions 2.13.x antérieures à la version 2.13.15 avec Xenial Stemcells antérieures à la version 621.376
- Tanzu Application Service for VMs versions 2.8.x avec Xenial Stemcells antérieures à la version 621.376
- Tanzu Application Service for VMs versions 2.9.x avec Xenial Stemcells antérieures à la version 621.376
- Tanzu Application Service for VMs versions 3.0.x antérieures à la version 3.0.7 avec Jammy Stemcells antérieures à la version 1.80
- Tanzu Application Service for VMs versions 4.0.x avec Jammy Stemcells antérieures à la version 1.80
- Tanzu Greenplum for Kubernetes versions antérieures à la version 2.0.0
- Tanzu RabbitMQ for VMs versions 2.2.x avec Jammy Stemcells antérieures à la version 1.80

Identificateurs externes

CVE-2016-10228 CVE-2017-11671 CVE-2017-12132 CVE-2019-25013 CVE-2020-27618
 CVE-2022-2345 CVE-2022-2581 CVE-2022-3099 CVE-2022-3256 CVE-2022-3324
 CVE-2022-3591 CVE-2022-38533 CVE-2022-41916 CVE-2022-43551 CVE-2022-43552
 CVE-2022-45061

Bilan de la vulnérabilité

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

Solution

Veuillez se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs.

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-5762-1>
- <https://tanzu.vmware.com/security/usn-5766-1>
- <https://tanzu.vmware.com/security/usn-5767-2>
- <https://tanzu.vmware.com/security/usn-5768-1>
- <https://tanzu.vmware.com/security/usn-5770-1>
- <https://tanzu.vmware.com/security/usn-5775-1>
- <https://tanzu.vmware.com/security/usn-5788-1>