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 dans les produits VMware
Numéro de Référence	41411804/23
Date de Publication	18 Avril 2022
Risque	Important
Impact	Important

Systèmes affectés

- Canonical Ubuntu 16.04
- Canonical Ubuntu 18.04
- Canonical Ubuntu 22.04
- Isolation Segment versions 2.11.x antérieures à 2.11.29
- Isolation Segment versions 2.12.x antérieures à 2.12.19
- Isolation Segment versions 2.13.x antérieures à 2.13.14
- Isolation Segment versions 3.0.x antérieures à 3.0.7 (avec Jammy Stemcells versions antérieures à 1.80)
- Operations Manager versions 2.10.x antérieures à 2.10.51
- Operations Manager versions 3.0.x antérieures à 3.0.4
- Platform Automation Toolkit versions 4.0.x antérieures à to 4.0.13
- Platform Automation Toolkit versions 4.1.x antérieures à 4.1.13
- Platform Automation Toolkit versions 4.2.x antérieures à 4.2.8
- Platform Automation Toolkit versions 4.3.x versions antérieures à 4.3.5
- Platform Automation Toolkit versions 4.4.x versions antérieures à 4.4.30
- Platform Automation Toolkit versions 5.0.x versions antérieures à 5.0.23
- Platform Automation Toolkit versions 5.1.x versions antérieures à 5.1.0
- Tanzu Greenplum for Kubernetes versions antérieures à 1.4.0
- VMware Tanzu Application Service for VMs versions 2.11.x antérieures à 2.11.35
- VMware Tanzu Application Service for VMs versions 2.12.x antérieures à 2.12.24
- VMware Tanzu Application Service for VMs versions 2.13.x antérieures à 2.13.17
- VMware Tanzu Application Service for VMs versions 3.0.x antérieures à 3.0.7 (avec Jammy Stemcells versions 1.80)

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

Identificateurs externes

- CVE-2021-23222 , CVE-2021-33621 , CVE-2021-3682 , CVE-2021-3750 , CVE-2021-3930 , CVE-2022-0216 , CVE-2022-0392 , CVE-2022-0417 , CVE-2022-24805 , CVE-2022-24806 , CVE-2022-24807 , CVE-2022-24808 , CVE-2022-24809 , CVE-2022-24810 , CVE-2022-2962 , CVE-2022-3165 , CVE-2022-33070 , CVE-2022-37454 , CVE-2022-40898 , CVE-2022-44617 , CVE-2022-44792 , CVE-2022-44793 , CVE-2022-45061 , CVE-2022-46285 , CVE-2022-47629 , CVE-2022-4883 , CVE-2023-22809

Bilan de la vulnérabilité

VMware annonce la correction de plusieurs vulnérabilités dans les produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'exécuter du code arbitraire, de réussir une élévation des privilèges, de causer un déni de service et de porter atteinte à la confidentialité des données.

Solution

Veuillez se référer au bulletin de sécurité VMware pour plus d'infirmation.

Risques

- Exécution du code arbitraire à distance
- Elévation de privilèges
- Déni de service
- Atteinte à la confidentialité des données

Annexe

Bulletin de sécurité VMware**:**

- https://tanzu.vmware.com/security/usn-5821-1
- https://tanzu.vmware.com/security/usn-5811-1
- https://tanzu.vmware.com/security/usn-5807-1
- https://tanzu.vmware.com/security/usn-5806-2
- https://tanzu.vmware.com/security/usn-5801-1
- https://tanzu.vmware.com/security/usn-5795-2
- https://tanzu.vmware.com/security/usn-5767-1
- https://tanzu.vmware.com/security/usn-5765-1