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	58712511/25
Date de Publication	25 Novembre 2025
Risque	Important
Impact	Important

Systèmes affectés

- VMware Tanzu pour Postgres on Tanzu Platform versions antérieures à 10.2.1
- Stemcells (Windows) versions antérieures à 2019.92.x
- Stemcells (Ubuntu Noble) versions antérieures à 1.126.x
- Stemcells (Ubuntu Jammy) versions antérieures à 1.954.x
- Stemcells (Ubuntu Jammy FIPS) versions antérieures à 1.954.x
- Stemcells (Ubuntu Jammy Azure Light) versions antérieures à 1.954.x
- Platform Services pour VMware Tanzu Platform versions antérieures à 10.3.1
- Metric Store versions antérieures à 1.8.1
- Isolation Segmentation pour VMware Tanzu Platform versions antérieures à 6.0.22
- Isolation Segmentation pour VMware Tanzu Platform versions antérieures à 10.3.1
- Isolation Segmentation pour VMware Tanzu Platform versions antérieures à 10.2.5
- Elastic Application Runtime pour VMware Tanzu Platform versions antérieures à 6.0.22
- Elastic Application Runtime pour VMware Tanzu Platform versions antérieures à 10.3.1
- Elastic Application Runtime pour VMware Tanzu Platform versions antérieures à 10.2.5
- Elastic Application Runtime Windows add-on pour VMware Tanzu Platform versions antérieures à 6.0.22
- Elastic Application Runtime Windows add-on pour VMware Tanzu Platform versions antérieures à 10.3.1
- Elastic Application Runtime Windows add-on pour VMware Tanzu Platform versions antérieures à 10.2.5
- App Metrics versions antérieures à 2.3.2
- AI Services pour VMware Tanzu Platform versions antérieures à 10.3.1

Identificateurs externes

- CVE-2025-9230 CVE-2025-8194 CVE-2025-8114 CVE-2025-64329
- CVE-2025-61795 CVE-2025-61748 CVE-2025-61725 CVE-2025-61724

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

- CVE-2025-61723 CVE-2025-6069 CVE-2025-5981 CVE-2025-59530
- CVE-2025-58189 CVE-2025-58188 CVE-2025-58187 CVE-2025-58186
- CVE-2025-58185 CVE-2025-58183 CVE-2025-58058 CVE-2025-53066
- CVE-2025-53057 CVE-2025-52881 CVE-2025-50182 CVE-2025-50181
- CVE-2025-49014 CVE-2025-47912 CVE-2025-47907 CVE-2025-47906
- CVE-2025-4674 CVE-2025-4673 CVE-2025-4517 CVE-2025-4516
- CVE-2025-4435 CVE-2025-4330 CVE-2025-4138 CVE-2025-40300
- CVE-2025-22874 CVE-2025-22872 CVE-2025-22871 CVE-2025-22870
- CVE-2025-22869 CVE-2025-22868 CVE-2025-22866 CVE-2025-13425
- CVE-2025-11226 CVE-2025-0938 CVE-2025-0913 CVE-2024-9287
- CVE-2024-9143 CVE-2024-8088 CVE-2024-7592 CVE-2024-7254
- CVE-2024-6923 CVE-2024-6345 CVE-2024-6232 CVE-2024-6119
- CVE-2024-5535 CVE-2024-51744 CVE-2024-50602 CVE-2024-4741
- CVE-2024-47081 CVE-2024-4603 CVE-2024-45341 CVE-2024-45337
- CVE-2024-45336 CVE-2024-4032 CVE-2024-35255 CVE-2024-34158
- CVE-2024-34156 CVE-2024-34155 CVE-2024-25621 CVE-2024-2511
- CVE-2024-24791 CVE-2024-24790 CVE-2024-24789 CVE-2024-13176
- CVE-2024-12718 CVE-2024-12254 CVE-2024-10979 CVE-2024-10978
- CVE-2024-10977 CVE-2024-10976 CVE-2023-27043 CVE-2022-40897
- CVE-2022-29526

Bilan de la vulnérabilité

VMware annonce la correction de plusieurs vulnérabilités affectant les produits VMware susmentionnés. L'exploitation de ces failles peut permettre à un attaquant de causer un déni de service, de contourner la politique de sécurité, de porter atteinte à la confidentialité des données et de prendre le contrôle du système affecté.

Solution :

Veuillez se référer au bulletin de sécurité VMware du 24 Novembre 2025 pour plus d'infirmation.

Risque :

- Déni de service ;
- Atteinte à la confidentialité des données ;
- Contournement de la politique de sécurité ;
- Prise de contrôle du système.

Annexe

Bulletin de sécurité VMware du 24 Novembre 2025**:**

- https://support.broadcom.com/web/ecx/security-advisory?segment=VT