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 critiques dans VMware Tanzu
Numéro de Référence	57903010/25
Date de Publication	30 Octobre 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- Tanzu pour Valkey versions 8.1.x antérieures à 8.1.4
- Tanzu pour Valkey versions 8.0.x antérieures à 8.0.6
- Tanzu pour Valkey versions 7.2.x antérieures à 7.2.11
- Tanzu pour Valkey versions 3.x antérieures à 3.2.0 sur Kubernetes
- Tanzu GemFire versions antérieures à 10.2.0
- Tanzu GemFire Management Console versions antérieures à 1.4.1

Identificateurs externes

- CVE-2016-1000027 CVE-2022-29458 CVE-2024-12798
- CVE-2024-6345 CVE-2024-6763 CVE-2025-11226
- CVE-2025-22227 CVE-2025-27151 CVE-2025-32414
- CVE-2025-32415 CVE-2025-4674 CVE-2025-46817
- CVE-2025-46818 CVE-2025-46819 CVE-2025-47273
- CVE-2025-47906 CVE-2025-47907 CVE-2025-49844
- CVE-2025-5115 CVE-2025-5222 CVE-2025-53864
- CVE-2025-54388 CVE-2025-55163 CVE-2025-58056
- CVE-2025-58057 CVE-2025-5914 CVE-2025-7425
- CVE-2025-8058 CVE-2025-8869

Bilan de la vulnérabilité

VMware annonce la correction de plusieurs vulnérabilités critiques affectant les versions susmentionnées de VMware Tanzu. L'exploitation de ces failles peut permettre à un attaquant de causer un déni de service, de contourner la politique de sécurité, de réussir une élévation de privilèges, de porter atteinte à la confidentialité des données et d'exécuter du code arbitraire à distance.

Solution :

Veuillez se référer au bulletin de sécurité VMware du 28 Octobre 2025 pour plus d'infirmation.

Risque :

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

Annexe

Bulletin de sécurité VMware du 28 Octobre 2025**:**

- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36258
- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36259
- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36260
- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36261
- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36262
- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36263
- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36264

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