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	61911203/26
Date de Publication	12 Mars 2026
Risque	Critique
Impact	Critique

Systèmes affectés

- Tanzu pour Valkey versions 7.2.x antérieures à 7.2.12 ;
- Tanzu pour Valkey versions 8.0.x antérieures à 8.0.7 ;
- Tanzu pour Valkey versions 8.1.x antérieures à 8.1.6 ;
- Tanzu pour Valkey versions 9.0.x antérieures à 9.0.3 ;

Identificateurs externes

- CVE-2005-2541 CVE-2022-27943 CVE-2022-3219 CVE-2022-41409 CVE-2023-2953
- CVE-2023-30571 CVE-2023-32636 CVE-2023-39804 CVE-2023-4156 CVE-2023-45322
- CVE-2023-50495 CVE-2024-0232 CVE-2024-11053 CVE-2024-13176 CVE-2024-34459
- CVE-2024-41996 CVE-2024-7264 CVE-2024-9681 CVE-2025-13151 CVE-2025-14017
- CVE-2025-14087 CVE-2025-14512 CVE-2025-14831 CVE-2025-15281 CVE-2025-1632
- CVE-2025-27113 CVE-2025-30258 CVE-2025-3360 CVE-2025-4674 CVE-2025-47906
- CVE-2025-47907 CVE-2025-47912 CVE-2025-5278 CVE-2025-58183 CVE-2025-58185
- CVE-2025-58186 CVE-2025-58187 CVE-2025-58188 CVE-2025-58189 CVE-2025-5915
- CVE-2025-5916 CVE-2025-5917 CVE-2025-5918 CVE-2025-60753 CVE-2025-6170
- CVE-2025-61723 CVE-2025-61724 CVE-2025-61725 CVE-2025-61726 CVE-2025-61727
- CVE-2025-61728 CVE-2025-61729 CVE-2025-61730 CVE-2025-61731 CVE-2025-61732
- CVE-2025-62813 CVE-2025-64118 CVE-2025-68119 CVE-2025-68121 CVE-2025-68972
- CVE-2025-7039 CVE-2025-9232 CVE-2025-9820 CVE-2026-0861 CVE-2026-0915
- CVE-2026-0988 CVE-2026-0989 CVE-2026-0990 CVE-2026-0992 CVE-2026-1484
- CVE-2026-1485 CVE-2026-1489 CVE-2026-1757 CVE-2026-2100 CVE-2026-22185
- CVE-2026-24883 CVE-2026-26960 CVE-2026-27171

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 11 Mars 2026 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 11 Mars 2026**:**

- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/37182
- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/37183
- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/37184
- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/37185
- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/37186

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: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma