



## BULLETIN DE SECURITE

|                            |                                            |
|----------------------------|--------------------------------------------|
| <b>Titre</b>               | Vulnérabilités critiques dans VMware Tanzu |
| <b>Numéro de Référence</b> | 57401310/25                                |
| <b>Date de Publication</b> | 13 Octobre 2025                            |
| <b>Risque</b>              | Critique                                   |
| <b>Impact</b>              | Critique                                   |

### Systèmes affectés

- VMware Tanzu pour MySQL sur Kubernetes version antérieure à 2.0

### Identificateurs externes

- CVE-2025-4802 CVE-2025-4673 CVE-2025-40909
- CVE-2025-3576 CVE-2025-30722 CVE-2025-30721
- CVE-2025-30715 CVE-2025-30705 CVE-2025-30704
- CVE-2025-30703 CVE-2025-30699 CVE-2025-30696
- CVE-2025-30695 CVE-2025-30693 CVE-2025-30689
- CVE-2025-30688 CVE-2025-30687 CVE-2025-30685
- CVE-2025-30684 CVE-2025-30683 CVE-2025-30682
- CVE-2025-30681 CVE-2025-29088 CVE-2025-27587
- CVE-2025-24528 CVE-2025-22871 CVE-2025-22866
- CVE-2025-21585 CVE-2025-21584 CVE-2025-21581
- CVE-2025-21580 CVE-2025-21579 CVE-2025-21577
- CVE-2025-21575 CVE-2025-21574 CVE-2025-21559
- CVE-2025-21555 CVE-2025-21546 CVE-2025-21540
- CVE-2025-21536 CVE-2025-21534 CVE-2025-21529
- CVE-2025-21525 CVE-2025-21523 CVE-2025-21522
- CVE-2025-21521 CVE-2025-21519 CVE-2025-21518
- CVE-2025-21505 CVE-2025-21504 CVE-2025-21503
- CVE-2025-21501 CVE-2025-21500 CVE-2025-21497
- CVE-2025-21494 CVE-2025-21492 CVE-2025-21491
- CVE-2025-21490 CVE-2025-0938 CVE-2025-0395
- CVE-2024-9287 CVE-2024-9143 CVE-2024-8096
- CVE-2024-8088 CVE-2024-6923 CVE-2024-6232

- CVE-2024-6119 CVE-2024-5642 CVE-2024-5535
- CVE-2024-50602 CVE-2024-4741 CVE-2024-4603
- CVE-2024-45492 CVE-2024-45491 CVE-2024-45490
- CVE-2024-45341 CVE-2024-45336 CVE-2024-4032
- CVE-2024-37371 CVE-2024-37370 CVE-2024-3596
- CVE-2024-34158 CVE-2024-34156 CVE-2024-34155
- CVE-2024-33602 CVE-2024-33601 CVE-2024-33600
- CVE-2024-33599 CVE-2024-2961 CVE-2024-28834
- CVE-2024-28182 CVE-2024-28085 CVE-2024-26461
- CVE-2024-26458 CVE-2024-2511 CVE-2024-24791
- CVE-2024-24790 CVE-2024-24789 CVE-2024-24787
- CVE-2024-24785 CVE-2024-24784 CVE-2024-24783
- CVE-2024-2398 CVE-2024-22365 CVE-2024-2236
- CVE-2024-21241 CVE-2024-21239 CVE-2024-21237
- CVE-2024-21236 CVE-2024-21231 CVE-2024-21230
- CVE-2024-21219 CVE-2024-21213 CVE-2024-21212
- CVE-2024-21207 CVE-2024-21201 CVE-2024-21200
- CVE-2024-21199 CVE-2024-21198 CVE-2024-21197
- CVE-2024-21196 CVE-2024-21194 CVE-2024-21193
- CVE-2024-21185 CVE-2024-21179 CVE-2024-21177
- CVE-2024-21173 CVE-2024-21171 CVE-2024-21166
- CVE-2024-21165 CVE-2024-21163 CVE-2024-21162
- CVE-2024-21160 CVE-2024-21159 CVE-2024-21157
- CVE-2024-21142 CVE-2024-21137 CVE-2024-21135
- CVE-2024-21134 CVE-2024-21130 CVE-2024-21129
- CVE-2024-21127 CVE-2024-21125 CVE-2024-21102
- CVE-2024-21096 CVE-2024-21087 CVE-2024-21069
- CVE-2024-21062 CVE-2024-21061 CVE-2024-21060
- CVE-2024-21057 CVE-2024-21056 CVE-2024-21055
- CVE-2024-21054 CVE-2024-21053 CVE-2024-21052
- CVE-2024-21051 CVE-2024-21050 CVE-2024-21049
- CVE-2024-21047 CVE-2024-21015 CVE-2024-21013
- CVE-2024-21009 CVE-2024-21008 CVE-2024-21000
- CVE-2024-20998 CVE-2024-20996 CVE-2024-20994
- CVE-2024-20993 CVE-2024-20985 CVE-2024-20984
- CVE-2024-20983 CVE-2024-20982 CVE-2024-20981
- CVE-2024-20978 CVE-2024-20977 CVE-2024-20976
- CVE-2024-20974 CVE-2024-20973 CVE-2024-20972
- CVE-2024-20971 CVE-2024-20970 CVE-2024-20969
- CVE-2024-20968 CVE-2024-20967 CVE-2024-20966
- CVE-2024-20965 CVE-2024-20964 CVE-2024-20963
- CVE-2024-20962 CVE-2024-20961 CVE-2024-20960
- CVE-2024-12747 CVE-2024-12243 CVE-2024-12133
- CVE-2024-12088 CVE-2024-12087 CVE-2024-12085

- CVE-2024-11168 CVE-2024-10041 CVE-2024-0727
- CVE-2024-0553 CVE-2024-0450 CVE-2023-7104
- CVE-2023-7008 CVE-2023-6918 CVE-2023-6597
- CVE-2023-6237 CVE-2023-6129 CVE-2023-6004
- CVE-2023-5981 CVE-2023-5678 CVE-2023-5363
- CVE-2023-5156 CVE-2023-48795 CVE-2023-4813
- CVE-2023-4807 CVE-2023-4806 CVE-2023-47038
- CVE-2023-4641 CVE-2023-46218 CVE-2023-45918
- CVE-2023-45290 CVE-2023-45289 CVE-2023-45288
- CVE-2023-45285 CVE-2023-44487 CVE-2023-4039
- CVE-2023-40217 CVE-2023-4016 CVE-2023-39804
- CVE-2023-39326 CVE-2023-39325 CVE-2023-39323
- CVE-2023-38546 CVE-2023-3817 CVE-2023-36054
- CVE-2023-3446 CVE-2023-2975 CVE-2023-2953
- CVE-2023-29383 CVE-2023-27043 CVE-2023-26604
- CVE-2023-2650 CVE-2023-24329 CVE-2023-22114
- CVE-2023-22112 CVE-2023-22103 CVE-2023-22097
- CVE-2023-22092 CVE-2023-22084 CVE-2023-22079
- CVE-2023-22078 CVE-2023-22070 CVE-2023-22068
- CVE-2023-22066 CVE-2023-22064 CVE-2023-22059
- CVE-2023-22032 CVE-2023-1255 CVE-2023-0466
- CVE-2023-0465 CVE-2023-0464 CVE-2023-0401
- CVE-2023-0286 CVE-2023-0217 CVE-2023-0216
- CVE-2023-0215 CVE-2022-48566 CVE-2022-48565
- CVE-2022-48564 CVE-2022-48560 CVE-2022-45061
- CVE-2022-4450 CVE-2022-4304 CVE-2022-4203
- CVE-2022-40735 CVE-2022-3996 CVE-2022-3786
- CVE-2022-3602 CVE-2022-3358 CVE-2022-2097
- CVE-2022-2068 CVE-2022-1473 CVE-2022-1434
- CVE-2022-1343 CVE-2022-1292 CVE-2022-0391
- CVE-2021-46848 CVE-2021-4189 CVE-2017-11164
- CVE-2016-2781 CVE-2016-20013 CVE-2013-4235

## 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 10 Octobre 2025 pour plus d'information.

## Risque :

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](mailto: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](mailto:contact@macert.gov.ma)

- 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 10 Octobre 2025:

- <https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36208>