



BULLETIN DE SECURITE

Titre	Vulnérabilités critiques dans VMware Tanzu
Numéro de Référence	59653012/25
Date de Publication	30 Décembre 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- AI Services pour VMware Tanzu Platform versions antérieures à 10.3.2 ;

Identificateurs externes

- CVE-2022-29526 CVE-2023-48022 CVE-2024-45337
- CVE-2024-7254 CVE-2025-0913 CVE-2025-22869
- CVE-2025-22874 CVE-2025-31133 CVE-2025-34351
- CVE-2025-4673 CVE-2025-4674 CVE-2025-47906
- CVE-2025-47907 CVE-2025-47910 CVE-2025-47912
- CVE-2025-48924 CVE-2025-52565 CVE-2025-52881
- CVE-2025-58183 CVE-2025-58185 CVE-2025-58186
- CVE-2025-58187 CVE-2025-58188 CVE-2025-58189
- CVE-2025-61723 CVE-2025-61724 CVE-2025-61725
- CVE-2025-61727 CVE-2025-61729 CVE-2025-62164
- CVE-2025-62372 CVE-2025-62426 CVE-2025-62593
- CVE-2025-62727 CVE-2025-66448

Bilan de la vulnérabilité

VMware annonce la correction de plusieurs vulnérabilités critiques affectant les services d'IA pour la plateforme 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 25 Décembre 2025 pour plus

d'information.

Risque :

- Dénî 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 25 Décembre 2025:

- <https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36640>