ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information
Centre de Veille de Détection et de Réaction aux Attaques Informatiques

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات
مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

BULLETIN DE SECURITE

Titre	Vulnérabilité critique affectant Veeam Backup
Numéro de Référence	52400602/25
Date de publication	06 Février 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- Veeam Updater versions antérieures à 9.0.0.1127 dans Veeam Backup pour Oracle Linux Virtualization Manager et Red Hat Virtualization versions 3, 4.0 et 4.1
- Veeam Updater versions antérieures à 7.9.0.1124 dans Veeam Backup pour Salesforce versions 3.1 et antérieures
- Veeam Updater versions antérieures à 9.0.0.1126 dans Veeam Backup pour AWS versions 6a et 7
- Veeam Updater versions antérieures à 9.0.0.1125 dans Veeam Backup pour Nutanix AHV versions 5.0 et 5.1
- Veeam Updater versions antérieures à 9.0.0.1128 dans Veeam Backup pour Google Cloud versions 4 et 5 et pour Microsoft Azure versions 5a et 6

Identificateurs externes

- CVE-2025-23114

Bilan de la vulnérabilité

Veeam annonce la correction d'une vulnérabilité critique affectant les versions susmentionnées de son produit « Veeam Updater ». L'exploitation de cette vulnérabilité peut permettre à un attaquant distant d'exécuter du code arbitraire.

Solution

Veuillez se référer au bulletin de sécurité de Veeam afin d'installer les nouvelles mises à jour.

Risque

- Exécution de code arbitraire à distance

Référence

Bulletin de sécurité Veeam :

- https://www.veeam.com/kb4712