GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA RÉPUBLIQUE DE VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

SERVICE DE COMMUNICATION ET DE TRANSFORMATION NUMÉRIQUE

SPR 9108 Port-Vila, Vanuatu
Tél : (678) 33380

1 June 2026

Avis 139 : Vulnérabilité de contrôle d'accès à granularité insuffisante dans Microsoft Defender (CVE-2026-33825).

Date de publication : 22 avril 2026
Degré d'impact : ÉLEVÉ / CRITIQUE
TLP : CLAIR

Le service de Communication et de Transformation numérique (SCTN), par l'intermédiaire du CERTVU publie l'avis suivant.

Cette alerte s'adresse aux organisations ainsi qu'aux administrateurs de systèmes et réseaux utilisant les produits mentionnés ci-dessus. Elle est destinée à être comprise par des utilisateurs techniques et des administrateurs de systèmes.

Objet de l'alerte

CVE-2026-33825 est une vulnérabilité de haute sévérité (CVSS ~8.6) dans VMware vCenter Server. Cette faille est causée par une validation insuffisante des entrées (CWE-20) au sein de certains points d'API exposés par vCenter Server.

Systèmes concernés

La vulnérabilité affecte :

- **VMware vCenter Server** (plusieurs versions antérieures aux mises à jour de sécurité 2026).
- Les deux types de déploiements :
  - vCenter Server Appliance (VCSA)
  - Déploiements vCenter sur Windows (hérités)

Environnements courants à risque :

- Plateformes de virtualisation d'entreprise
- Infrastructures de cloud privé
- Centres de données gérant des hôtes VMware ESXi

Étant donné que vCenter gère de manière centralisée l'infrastructure virtuelle, il constitue une cible de grande valeur.

Implications

L'exploitation est distante et basée sur le réseau, nécessitant uniquement un accès HTTP.

Chaîne d'attaque typique :

1. **Identification de la cible**
   - Les attaquants recherchent des instances vCenter exposées (ports 443/5480).
2. **Requête API spécialement conçue**
   - Requêtes malveillantes envoyées aux points de terminaison vulnérables de l'API vCenter.
3. **Validation d'entrée incorrecte déclenchée**
   - Le serveur ne parvient pas à nettoyer ou valider les données entrantes.
4. **Contournement des contrôles de sécurité**
   - L'attaquant manipule la logique de traitement des requêtes pour obtenir un accès non autorisé.
5. **Exécution de code à distance (dans les cas avancés)**
   - Dans certains scénarios, les attaquants peuvent exécuter des commandes arbitraires sur le serveur vCenter.

L'exploitation réussie de cette vulnérabilité peut permettre aux attaquants de :

- Obtenir un accès non autorisé au serveur vCenter.
- Exécuter des commandes ou du code arbitraire.
- Prendre le contrôle des machines virtuelles et des hôtes ESXi.
- Accéder à des données sensibles de l'infrastructure.
- Déployer des logiciels malveillants ou des ransomwares dans les environnements virtuels.
- Perturber les services ou arrêter des systèmes critiques.

Étant donné que vCenter contrôle l'ensemble de l'infrastructure virtuelle, une compromission peut entraîner une **prise de contrôle complète du centre de données**.

Mesures d'atténuation

CERTVU recommande les mesures suivantes :

1. Appliquer les mises à jour de sécurité VMware (Critique)

- Mettre à niveau vers les versions corrigées de VMware vCenter Server publiées dans les avis de sécurité de 2026.
- S'assurer que toutes les instances de vCenter sont mises à jour immédiatement.

2. Restreindre l’exposition de l’interface de gestion

- Ne pas exposer directement les interfaces de gestion de vCenter à Internet
- Restreindre l’accès via :
    - VPN
    - Hôtes bastion
    - Listes d’autorisation de pare-feu

Références

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2026-33825
3. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33825

.