**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 REPUBLIQUE DE VANUATU**

BUREAU DU PREMIER MINISTRE

CERTVU

SERVICE DE COMMUNICATION ET DE TRANSFORMATION NUMÉRIQUE

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

9 septembre 2025

**Avis 94 : Trend Micro Apex One (CVE-2025-54948)**
**Date de publication :** 18 août 2025
**Degré d'impact :** ÉLEVÉ / CRITIQUE
**TLP :** CLAIR

CERT Vanuatu (CERTVU) et le service de Communication et de Transformation (SCTN) numérique publient la présente alerte.

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

# Objet de l'alerte

CVE-2025-54948 est une vulnérabilité **critique d'exécution de code à distance (RCE)** dans la **console de gestion Trend Micro Apex One sur site**, qui permet à des attaquants distants pré-authentifiés de mettre à jour du code malveillant et d'exécuter des commandes système. Il résulte d'une injection de commande OS (faille CW-78_ due à une validation insuffisante des entrées dans la console de gestion.

# Systèmes concernés

Versions affectées ;

- Console de gestion Trend Micro Apex One (sur site) – plus précisément la version 2019 (14.0), y compris la version de Management Server 14039 et les versions antérieures.
- Trend Micro Apex One en tant que service (Cloud/SaaS) et Trend Vision One Endpoint Security (protection standard des terminaux) ont été initialement affectés, mais ont été automatiquement corrigés sans intervention nécessaire de la part des clients.

# Implication

Cette vulnérabilité pourrait permettre à un attaquant distant de télécharger du code malveillant et d'exécuter des commandes sur les installations affectées.

# Mesures d’atténuation

Le correctif critique (SP1 CP B14081) est disponible. Il s'agit d'une solution permanente qui rétablit la fonctionnalité de l'agent d'installation à distance.

Limitez l'accès à la console Apex One, particulièrement si son adresse IP est exposée à l'extérieur. Instaurez des restrictions au niveau du réseau ou des règlements de pare-feu pour limiter les interfaces accédant à la console.

Veuillez consulter ce lien pour plus d’informations sur les mesures d’atténuations et solutions : More information on the Mitigation and solution.

# Références


1. https://www.cve.org/CVERecord?id=CVE-2025-54948
2. https://success.trendmicro.com/en-US/solution/KA-0020652