**GOVERNMENT OF THE REPUBLIC OF VANUATU**

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PMB 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

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

13 janvier 2026

**Avis 110 : Vulnérabilité d'écriture hors limites dans WatchGuard Firebox**

**Date de publication :** 12 novembre 2025
**Degré d'impact :** ÉLEVÉ / CRITIQUE
**TLP :** CLAIR

Le service de Communication et de Transformation numérique (SCTN par l'intermédiaire du CERT Vanuatu (CERTVU)), publie la présente alerte.

Cette alerte s'adresse aux organisations et administrateurs de système/réseau 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-2025-9242** – Il s'agit d'une *faille d'écriture hors limites* dans le service IKEv2 du système d'exploitation WatchGuard Firewall OS. Un attaquant distant sans authentification requise peut exploiter cette faille pour exécuter du code arbitraire sur l'appareil.

# Systèmes concernés

Versions affectées :

- Les versions de Firewall OS suivantes sont concernées : Versions 11.10.2 à 11.12.4_update1, 12.0 à 12.11.13 et 2025.1
- La vulnérabilité affecte spécifiquement les configurations où l'appareil est utilisé pour :
    1. Le VPN pour Utilisateurs Mobiles utilisant IKEv2.
    2. Le VPN de Succursale utilisant IKEv2 avec un *pair de passerelle dynamique*.

# Implication

Les attaquants peuvent exploiter cette vulnérabilité des manières suivantes (vecteur d'attaque):

- L'attaquant cible le service VPN IKEv2 (généralement accessible à la périphérie du réseau) et déclenche la faille en envoyant une charge utile IKE AUTH ou un certificat spécialement conçu qui provoque un débordement de la mémoire tampon.
- L'exécution a lieu avant l'authentification (c'est-à-dire que l'attaquant n'a pas besoin d'informations d'identification valides), de sorte que l'appareil peut être compromis lorsqu'il est exposé au trafic externe.
- Une fois que l'attaquant a pris le contrôle de l'appareil, il peut pivoter vers le réseau interne, intercepter le trafic VPN, installer des portes dérobées persistantes ou faciliter l'exfiltration de données/ransomware. Étant donné que l'appareil se trouve à la périphérie du réseau, une compromission totale du réseau est plausible.

# Mesures d'atténuation

Le CERTVU recommande les mesures suivantes:

Correctif immédiat – Appliquez le correctif publié par le fournisseur :

- Pour la branche 12.x : passez à la version 12.11.4 (ou la version corrigée équivalente)
- Pour la branche 2025.1 : passez à la version 2025.1.1 (ou supérieure)
- Remarque : ne vous fiez pas aux versions en fin de vie (par exemple, la branche 11.x) pour assurer une sécurité continue.

Si le correctif ne peut pas être appliqué immédiatement :

- Limitez l'accès IKEv2/UDP 500 et UDP 4500 aux seuls points de terminaison de confiance.
- Désactivez les configurations VPN inutilisées (en particulier les configurations de pairs de passerelle dynamique).
- Surveillez les indicateurs d'exploitation : charge utile IKE_AUTH importante.

# Références


1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2025-9242