ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Vulnérabilité critique dans WatchGuard Firebox
Numéro de Référence	59471912/25
Date de Publication	19 Décembre 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- WatchGuard Firebox utilisant Fireware OS 2025.1 version antérieure à 2025.1.4 ;
- WatchGuard Firebox utilisant Fireware OS 12.x version antérieure à 12.11.6 ;
- WatchGuard Firebox utilisant Fireware OS 12.5.x (modèles T15 & T35) version antérieure à 12.5.15 ;
- WatchGuard Firebox utilisant Fireware OS 12.3.1 (version certifiée FIPS) version antérieure à 12.3.1_Update4 (B728352) ;
- WatchGuard Firebox utilisant Fireware OS 11.x Fin de vie (EoL) ;

La vulnérabilité impacte les appliances Firebox exécutant des versions vulnérables de Fireware OS, lorsqu'elles sont configurées avec :

- Mobile User VPN utilisant IKEv2;
- Branch Office VPN utilisant IKEv2;
- Pairs de passerelle dynamiques (dynamic gateway peers) ;

Identificateurs externes

- CVE-2025-14733;

Bilan de la vulnérabilité

WatchGuard a publié une alerte de sécurité concernant une vulnérabilité critique affectant le processus « iked de Fireware OS » sur les appliances WatchGuard Firebox. Cette faille permet à un attaquant distant non authentifié d'exécuter du code arbitraire lors de l'établissement des connexions VPN IKEv2, notamment lorsque des passerelles dynamiques sont ou ont été configurées.

WatchGuard confirme que cette vulnérabilité est activement exploitée, ce qui accroît significativement le risque de compromission des équipements exposés.

Solution

Veuillez se référer au bulletin de sécurité WatchGuard du 18 Décembre 2025 pour plus d'information.

En cas de suspicion ou de confirmation d'exploitation :

- Renouveler les clés pré-partagées VPN (PSK) ;
- Regénérer l'ensemble des certificats ;
- Réinitialiser tous les identifiants stockés localement ;

Risque

- Exécution de code arbitraire à distance ;
- Compromission complète de l'appliance ;
- Accès non autorisé aux communications VPN ;
- Compromission des identifiants et des clés cryptographiques;

Indices de compromission :

Les adresses IP suivantes ont été directement associées à des tentatives d'exploitation :

IP :

- 45.95.19[.]50 ;
- 51.15.17[.]89 ;
- 172.93.107[.]67 ;
- 199.247.7[.]82 ;

Annexe

Bulletin de sécurité WatchGuard 18 Décembre 2025:

- https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00027