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 DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

14 September 2026

Advisory 312: WatchGuard Fireware OS IKEv2 VPN "iked" Out-of-Bounds Write Leading to Unauthenticated Remote Code Execution - Actively Exploited (CVE-2025-14733).

Release Date: 12th September 2026
Impact: CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that operate a WatchGuard Firebox appliance with Mobile User VPN or Branch Office VPN configured over IKEv2. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2025-14733 is a critical, unauthenticated remote code execution vulnerability in the "iked" process of WatchGuard Fireware OS, publicly disclosed by WatchGuard on 19 December 2025 (WatchGuard Security Advisory WGSA-2025-00027) after active exploitation was already underway. The flaw affects IKEv2 processing for both Mobile User VPN and Branch Office VPN when configured with dynamic gateway peers.

What are the systems affected?

The following version(s) are affected:

- Fireware OS 11.10.2 through 11.12.4_Update1 (end-of-life, no patch available), 12.0 through 12.11.5, 12.5.x (T15/T35 models) through 12.5.14, and 2025.1 through 2025.1.3 - (Affected)

Fireware OS 2025.1.4, 12.11.6, 12.5.15 (T15/T35 models), and 12.3.1_Update4 (FIPS-certified) and later - (Not affected, patched)

Upgrade Fireware OS to the fixed version for your branch (2025.1.4, 12.11.6, 12.5.15, or 12.3.1_Update4) without delay, per WatchGuard Security Advisory WGSA-2025-00027.

What does this mean?

Typical attack flow:

1. **Send a crafted IKE_AUTH request to the Firebox's IKEv2 VPN service**
    - A remote, unauthenticated attacker sends a specially crafted IKE_AUTH request to a Firebox configured for Mobile User VPN or Branch Office VPN with dynamic gateway peers over IKEv2.
2. **Trigger an out-of-bounds write and execute arbitrary code**
    - The crafted request triggers an out-of-bounds write in the "iked" process, allowing the attacker to execute arbitrary code on the Firebox appliance without any authentication.

Attack vectors:

- A network-based, unauthenticated attack against any WatchGuard Firebox with Mobile User VPN or Branch Office VPN configured over IKEv2 with dynamic gateway peers, reachable from an untrusted network - most critically the public internet.
- No user interaction or privileges are required. This is confirmed under active exploitation from the moment of disclosure, is listed in CISA's KEV catalog, and continues to be flagged in Shadowserver's internet-wide scanning feed. This is not a theoretical risk, and any unpatched, internet-reachable Firebox should be treated as a plausible target.

Successful exploitation may allow attackers to:

- Execute arbitrary code on a WatchGuard Firebox appliance, without any authentication, via a single crafted IKEv2 request.
- Compromise the perimeter firewall/VPN gateway itself and use it as a foothold to intercept or manipulate traffic, and pivot into the wider internal network the Firebox protects.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor patch immediately

- Upgrade Fireware OS to 2025.1.4, 12.11.6, 12.5.15, or 12.3.1_Update4 (matching your current branch) as an emergency change, given confirmed active exploitation.

2. Restrict or disable IKEv2 VPN with dynamic gateway peers where patching must be delayed

Report any suspected compromise of a WatchGuard Firebox appliance to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://www.cve.org/CVERecord?id=CVE-2025-14733
2. https://github.com/advisories/GHSA-hv82-jj64-jf47