

**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

10 September 2026

**Advisory 296: WatchGuard Fireware OS Second Critical Out-of-Bounds Write in IKEv2 VPN - Confirmed Active Exploitation (CVE-2025-14733).**

**Release Date:** 9<sup>th</sup> September 2026

**Impact:** **CRITICAL**

**TLP:** CLEAR

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

This advisory is relevant to system and network administrators who operate WatchGuard Firebox firewall and VPN appliances, particularly those with Mobile User VPN or Branch Office VPN configured using IKEv2. This alert is intended primarily for a technical audience.

## What is it?

CVE-2025-14733 is a second, distinct critical out-of-bounds write vulnerability (CWE-787) in the iiked process of WatchGuard's Fireware OS, discovered internally by WatchGuard and disclosed on 18 December 2025 - a separate flaw from CVE-2025-9242 (see Advisory 295), affecting the same underlying VPN service. It again affects both the Mobile User VPN with IKEv2 and the Branch Office VPN using IKEv2 when configured with a dynamic gateway peer, allowing a remote, unauthenticated attacker to execute arbitrary code with no user interaction required.

CERTVU's own Shadowserver scan data for Vanuatu recorded scan hits tagged to this CVE, indicating vulnerable WatchGuard Firebox devices are present within Vanuatu's own network space therefore this advisory is issued on that basis.

## What are the systems affected?

The following version(s) are affected:

- WatchGuard Fireware OS 11.10.2 up to and including 11.12.4\_Update1, 12.0 and higher, and 2025.1 and higher - (Affected)

Fireware OS 2025.1.4, 12.11.6, 12.5.15 (T15/T35 models), and 12.3.1\_Update4 (FIPS) and later - (Not affected, patched); Fireware OS 11.x is end-of-life and does not receive a fix

As with CVE-2025-9242 (Advisory 295), a Firebox device may remain vulnerable even if the affected dynamic-gateway-peer VPN configuration has since been removed, if a Branch Office VPN to a static gateway peer is still configured. Administrators should confirm the installed Fireware OS version directly on each device rather than assuming an update has applied.

## What does this mean?

### Typical attack flow:

1. **Identify an internet-facing WatchGuard Firebox with IKEv2 VPN configured**
  - As with CVE-2025-9242 (Advisory 295), the device may have Mobile User VPN with IKEv2 or a Branch Office VPN using IKEv2 with a dynamic gateway peer configured, or remain vulnerable via a residual static gateway peer BOVPN.
2. **Send malformed IKEv2 messages to trigger the out-of-bounds write**
  - WatchGuard has observed exploitation attempts from specific attacker-controlled IP addresses in the wild. Malformed messages can cause the ikev2 process to crash or hang, interrupting VPN service, or depending on the crafted payload, this can lead to remote code execution and full compromise of the device, including traffic interception and credential theft.

### Attack vectors:

- A network-based attack against the IKEv2 VPN service, requiring no authentication and no user interaction, confirmed exploited as part of a wider campaign against edge devices and VPN gateways across multiple vendors.

## Mitigation process

CERTVU recommends the following:

1. Apply WatchGuard's security update immediately
  - Update Fireware OS to 2025.1.4, 12.11.6, 12.5.15 (T15/T35), or 12.3.1\_Update4 (FIPS) as appropriate for the device model, without delay. WatchGuard has confirmed this vulnerability is being actively exploited, so this should be treated as an emergency change.
2. Devices on end-of-life Fireware OS 11.x must be upgraded or replaced immediately and treated as potentially compromised until then
3. Rotate locally stored secrets on affected devices after patching
4. Apply temporary mitigations only if immediate patching is not possible

Report any suspected compromise arising from these vulnerabilities to CERTVU at [incident@cert.gov.vu](mailto:incident@cert.gov.vu) or on telephone (678) 33380.

## Reference

1. <https://www.cve.org/CVERecord?id=CVE-2025-14733>
2. <https://thehackernews.com/2025/12/watchguard-warns-of-active-exploitation.html>
3. <https://socprime.com/blog/cve-2025-14733-vulnerability/>
4. <https://www.cybersecuritydive.com/news/watchguard-critical-flaw-firebox-exploitation/808617/>