

**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 295: WatchGuard Fireware OS Critical Out-of-Bounds Write in IKEv2
VPN Leading to Unauthenticated Remote Code Execution (CVE-2025-9242).**

Release Date: 9th 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-2025-9242 is a critical out-of-bounds write vulnerability (CWE-787) in the iked process of WatchGuard's Fireware OS, the operating system running on WatchGuard Firebox firewall and VPN appliances. It affects both the Mobile User VPN with IKEv2 and the Branch Office VPN using IKEv2 when configured with a dynamic gateway peer, and allows a remote, unauthenticated attacker to execute arbitrary code on the device.

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 up to and including 12.11.3, and 2025.1 - (Affected)

Fireware OS versions specified in WatchGuard advisory WGSA-2025-00015 and later - (Not affected, patched). Fireware OS 11.x is end-of-life and does not receive a fix

What does this mean?

Typical attack flow:

1. **Identify an internet-facing WatchGuard Firebox with IKEv2 VPN configured**
 - The device may have Mobile User VPN with IKEv2 or a Branch Office VPN using IKEv2 with a dynamic gateway peer configured or may still be vulnerable via a static gateway peer BOVPN even if the dynamic configuration was removed.
2. **Send crafted IKEv2 packets to trigger the out-of-bounds write**
 - No authentication or user interaction is required. Successful exploitation grants remote code execution within the ikev2 process, which can lead to a persistent shell on the device, theft of the device's configuration and stored VPN credentials, and the ability to intercept or decrypt VPN traffic passing through the appliance.

Attack vectors:

- A network-based attack against the IKEv2 VPN service, requiring no authentication and no user interaction - directly reachable by any attacker able to send packets to the affected VPN service.

Indicators of Compromise:

Successful exploitation may allow attackers to:

- Achieve full compromise of the Firebox appliance, including persistent access, configuration theft, and VPN credential exposure.
- Intercept or decrypt VPN traffic and pivot from the compromised perimeter device into the internal network it was protecting.

Mitigation process

CERTVU recommends the following:

1. Apply WatchGuard's security update immediately
 - Update Fireware OS to a fixed version per WatchGuard advisory WGSA-2025-00015 without delay. Given confirmed active exploitation and confirmed local exposure, this should be treated as an emergency change.
2. Devices on end-of-life Fireware OS 11.x must be upgraded or replaced, as no fix is available for that branch
3. Apply temporary mitigations if immediate patching is not possible
4. Audit affected devices for signs of prior compromise

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

Reference

1. <https://www.cve.org/CVERecord?id=CVE-2025-9242>
2. <https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00015>
3. <https://www.infosecurity-magazine.com/news/watchguard-fireware-os-flaw/>