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 313: WatchGuard Fireware OS IKEv2 VPN "ike2_ProcessPayload_CERT" Stack Buffer Overflow ("yIKEs") - Actively Exploited in Ransomware Attacks (CVE-2025-9242).

Release Date: 12th September 2025
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 IKEv2 VPN services enabled. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2025-9242 - dubbed "yIKEs" by the discovering researchers at watchTowr Labs, is a critical, pre-authentication remote code execution vulnerability in the IKEv2 VPN service of WatchGuard Fireware OS, disclosed in September 2025. CERTVU is issuing this advisory now because CVE-2025-9242 continues to appear in Shadowserver Foundation internet-wide scanning data, which CERTVU monitors on a recurring basis. See also Advisory 312, CVE-2025-14733, disclosed roughly three months later in the same VPN component, a clear vendor-specific trend that makes this specific feature (IKEv2 VPN processing) worth a standing audit item rather than a one-off patch.

What are the systems affected?

The following version(s) are affected:

- Fireware OS 11.10.2 through 11.12.4_Update1, 12.0 through 12.11.3, and 2025.1 - (Affected)

Fireware OS 12.11.4 and later - (Not affected, patched)

Upgrade Fireware OS to version 12.11.4 or later without delay.

What does this mean?

Typical attack flow:

1. **Send a crafted identification payload during IKE_SA_AUTH negotiation**
    - A remote, unauthenticated attacker sends a maliciously crafted identification payload exceeding the expected 512-byte stack buffer to a Firebox's IKEv2 VPN service during IKE_SA_AUTH negotiation.
2. **Overflow the stack buffer and achieve root-level remote code execution**
    - The oversized payload overflows the stack buffer in the "ike2_ProcessPayload_CERT" function; in the absence of modern exploit mitigations on the affected binary, this allows the attacker to achieve arbitrary code execution with root-level privileges, as demonstrated by watchTowr Labs using a reverse Python shell.

Attack vectors:

- A network-based, unauthenticated, pre-authentication attack against any WatchGuard Firebox with IKEv2 VPN services reachable from an untrusted network - most critically the public internet.
- No user interaction or privileges are required.

Successful exploitation may allow attackers to:

- Execute arbitrary code with root-level privileges on a WatchGuard Firebox appliance, without any authentication, via a single crafted IKEv2 payload.
- Compromise the perimeter firewall/VPN gateway itself and use it to deploy ransomware or pivot further into the wider internal network the Firebox protects both consistent with confirmed real-world attack activity against this specific flaw.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor patch immediately

- Upgrade Fireware OS to version 12.11.4 or later as an emergency change, given confirmed active exploitation including in ransomware attacks.

2. Disable IKEv2 VPN services entirely where patching must be delayed
3. Audit for the related, separately-tracked IKEv2 vulnerability (CVE-2025-14733) on the same devices.

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-2025-9242
2. https://labs.watchtowr.com/yikes-watchguard-fireware-os-ikev2-out-of-bounds-write-cve-2025-9242/