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

24 November 2025

Advisory 110: WatchGuard Firebox Out-of-Bounds Write Vulnerability

Release Date: 12th of November 2025
Impact: HIGH / CRITICAL
TLP: CLEAR

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

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2025-9242 – is an *out-of-bound write* flaw in the IKEv2 daemon of WatchGuard Firewall OS. A remote attacker with no authentication required may exploit the flaw to execute arbitrary code on the device.

What are the Systems affected?

Affected:

- Firewall OS Versions 11.10.2 through 11.12.4_update1, 12.0 through 12.11.13 and 2025.1 are in scope.
- The vulnerability specifically impacts configurations where the device is used for:
  1. Mobile User VPN using IKEv2
  2. Branch Office VPN IKEv2 *with a dynamic gateway peer*

What does this mean?

How attackers exploit this vulnerability (attack vector)

- The attacker targets the IKEv2 VPN service (typically reachable at the network edge) and triggers the flaw by sending a specifically crafted IKE AUTH or certificate payload that causes the buffer write to overrun
- Execution occurs pre-authentication (i.e., attacker does not need valid credential) so the device can be compromised while exposed to external traffic.
- Once the attacker gains control of the appliance, they can pivot into the internal network, intercept VPN traffic, install persistent backdoors, or facilitate data exfiltration/ransomware. Given that the appliance is at the network boundary, full network compromise is plausible.

Mitigation process

CERTVU recommend:

Immediate Patching – Apply the vendor released patch:

- For 12.x branch: upgrade to version **12.11.4** (or the equivalent fixed version)
- For 2025.1 branch: upgrade to **2025.1.1** (or higher)
- Note: Do *not* rely on end-of-life versions (e.g., 11.x branch) for ongoing security.

If patching cannot be immediately deployed:

- Restrict IKEv2/UDP 500 and UDP 4500 access to trusted endpoints only.
- Disable unused VPN configurations (especially dynamic gateway peer setups).
- Monitor for indicators of exploitation: Large IKE_AUTH payload.

Reference

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2025-9242