Computer Emergency Response Team of Mauritius
Ministry of Information Technology, Communication and Innovation

CERT-MU Vulnerability Note

Critical WatchGuard Firebox Vulnerability Exposes 75,000+ Devices to Remote Code Execution

Vulnerability Note: VN-2025-42

Date of Issue: 22 October 2025

Severity Rating: High

Systems Affected:

WatchGuard Firebox appliances using IKEv2 VPNs with dynamic gateway peers on versions:

- 11.10.2 through 11.12.4_Update1
- 12.0 through 12.11.3
- 2025.1

Description

A critical remote code execution vulnerability (CVE-2025-9242) affecting WatchGuard Firebox network security appliances has left approximately 75,835 devices exposed to potential attacks. The vulnerability, discovered by security researchers and disclosed by WatchGuard on September 17, 2025, has a CVSS severity score of 9.3 (Critical).

The security issue is an out-of-bounds write vulnerability in the Fireware OS 'iked' process, which handles IKEv2 VPN negotiations. Attackers can exploit this flaw without authentication by sending specially crafted IKEv2 packets to vulnerable Firebox endpoints, forcing the device to write data to unintended memory areas. This could allow remote attackers to execute arbitrary code on affected devices.

Recent scans conducted by The Shadowserver Foundation on October 19, 2025, revealed that 75,835 Firebox appliances remain vulnerable worldwide, with the highest concentrations in the United States (24,500), Germany (7,300), Italy (6,800), United Kingdom (5,400), Canada (4,100), and France (2,000). These figures represent real deployments rather than honeypots, indicating widespread exposure.

While no active exploitation of CVE-2025-9242 has been reported yet, the critical nature of the vulnerability and the large number of exposed devices make this an urgent security concern for organizations using WatchGuard Firebox appliances.

CVE Information

CVE-2025-9242 (WatchGuard Fireware OS Out-of-Bounds Write - CVSS 9.3):

NVD Details

Bleeping Computer Report

Shadowserver Foundation Data

WatchGuard Security Bulletin

Mitigation

WatchGuard recommends the following immediate actions:

1. Critical Patching: Upgrade to one of the following patched versions:

- 2025.1.1
- 12.11.4
- 12.5.13
- 12.3.1_Update3 (B722811)

2. End-of-Life Versions: Note that version 11.x has reached end of support and will not receive security updates. Administrators using these versions should migrate to supported versions immediately.

3. Temporary Workaround: For devices configured only with Branch Office VPNs to static gateway peers, implement additional security measures by securing the connection using IPSec and IKEv2 protocols according to WatchGuard documentation.

4. Network Segmentation: Consider isolating Firebox appliances from direct internet exposure where possible, especially for devices that cannot be immediately patched.

5. Monitoring: Implement network monitoring to detect any unusual IKEv2 traffic patterns that might indicate exploitation attempts.

Postal address
Mauritian Computer Emergency Response Team (CERT-MU)
Ministry of Information Technology, Communication and Innovation
2nd Floor, Wing A,
Shri Atal Bihari Vajpayee Tower,
Cybercity Ebene