

CVE-2025-14733

WatchGuard Firebox Out of Bounds Write Vulnerability

Exigent

CISA KEV since Dec 19, 2025

Actively exploited

Ransomware use known

An Out-of-bounds Write vulnerability in the WatchGuard Fireware OS iked process may allow a remote unauthenticated attacker to execute arbitrary code. This vulnerability affects both the mobile user VPN with IKEv2 and the branch office VPN using IKEv2 when configured with a dynamic gateway peer. If the Firebox was previously configured with the mobile user VPN with IKEv2 or a branch office VPN using IKEv2 to a dynamic gateway peer, and both of those configurations have since been deleted, that Firebox may still be vulnerable if a branch office VPN to a static gateway peer is still configured.

EVRS 85/100 Immediate priority	CVSS V4.0 9.3 Critical · NVD	EPSS 0.265 98th percentile · FIRST	CISA DEADLINE Dec 26, 2025 CISA federal deadline · Overdue by 10 months
--	--	--	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☒ Ransomware	Known ransomware campaigns	☐ KEV recency	Added to CISA KEV within the last year
☒ EPSS	0.265 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.3	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable. **CISA note:** Check for signs of potential compromise on all internet accessible instances after applying mitigations.

Basis: CISA KEV required action

Affected and fixed versions · 31 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
fireware	≥ 11.10.2 < 12.5.15 ≥ 11.10.2 < 12.11.6 ≥ 2025.1 < 2025.1.4	12.5.15 · 12.11.6 · 2025.1.4	NVD
firebox t15	—	no fixed version listed	NVD
firebox t35	—	no fixed version listed	NVD
firebox m270	—	no fixed version listed	NVD
firebox m290	—	no fixed version listed	NVD
firebox m370	—	no fixed version listed	NVD
firebox m390	—	no fixed version listed	NVD
firebox m440	—	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-hv82-jj64-jf47

Additional guidance watchguard.com/wgrd-psirt/advisory/wgsa-2025-00027

NVD nvd.nist.gov/vuln/detail/CVE-2025-14733

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2025-204437

Current data evulnable.com/vulnerability-management/cve/CVE-2025-14733

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.