

CVE-2022-23176

WatchGuard Firebox and XTM Privilege Escalation Vulnerability

CISA KEV since Apr 11, 2022

Actively exploited

WatchGuard Firebox and XTM appliances allow a remote attacker with unprivileged credentials to access the system with a privileged management session via exposed management access. This vulnerability impacts Fireware OS before 12.7.2_U1, 12.x before 12.1.3_U3, and 12.2.x through 12.5.x before 12.5.7_U3.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 8.8 High · NVD	EPSS 0.108 95.8th percentile · FIRST	CISA DEADLINE May 2, 2022 KEV since 2022 · listed over a year
---	---------------------------------------	---	--

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	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.108 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified**CISA required action:** Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
fireware	≥ 12.0.0 < 12.1.3 ≥ 12.2.0 < 12.5.7 12.1.3 12.5.7 12.7.2	12.1.3 · 12.5.7	NVD

Sources

Vendor guidance	securityportal.watchguard.com	NVD	nvd.nist.gov/vuln/detail/CVE-2022-23176
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2022-28267
Current data	evulnable.com/vulnerability-management/cve/CVE-2022-23176		

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