مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in WatchGuard Firebox Fireware OS Web UI

Tracking #:432318710

Date:02-04-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a path traversal vulnerability in the Fireware OS Web UI of WatchGuard Firebox devices that may allow a privileged authenticated attacker to write arbitrary files and execute code with elevated privileges, potentially compromising system confidentiality, integrity, and availability.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE:** CVE-2026-3987
- **Severity:** High **CVSS v4.0 Score:** 8.6
- Insufficient input validation in the Fireware Web UI allows a privileged attacker to perform a path traversal attack, leading to arbitrary file writes. This may escalate to remote code execution under an elevated system context.

Affected Products

- **Fireware OS 12.x:** Versions 12.6.1 through 12.11.8 on Firebox models including T20, T25, T40, T45, T55, T70, T80, T85, M270, M290, M370, M390, M470, M570, M590, M670, M690, M440, M4600, M4800, M5600, M5800, Firebox Cloud, Firebox NV5, FireboxV.
- **Fireware OS 2025.1.x:** Versions 2025.1 through 2026.1.2 on Firebox models including T115-W, T125, T125-W, T145, T145-W, T185, M295, M395, M495, M595, M695.

Fixed Versions

- **Fireware OS 12.x:** 12.12 or later
- **Fireware OS 2025.1.x:** 2026.2 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by WatchGuard.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2026-00009