AUTORITETI KOMBËTAR

PËR SIGURINË KIBERNETIKE

Dobësi me Rrezikshmëri të Lartë në WatchGuard Firebox Fireware OS Web UI

Data: 03/04/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive

Është identifikuar një dobësi path traversal në Fireware OS Web UI që mund të lejojë shkrim të skedarëve arbitrarë dhe ekzekutim kodi me privilegje të larta.

Informacione Teknike

Detaje të Dobësisë:

- **CVE:** CVE-2026-3987
- **Rrezikshmëria:** E lartë (CVSS v4.0: 8.6)

Validimi i pamjaftueshëm i input-it në Fireware Web UI i lejon një sulmuesi me privilegje të kryejë një sulm **path traversal**, duke mundësuar shkrimin e skedarëve arbitrarë. Kjo mund të përshkallëzohet në ekzekutim kodi në distancë në një kontekst sistemi me privilegje të ngritura.

Produktet e Prekura

- **Fireware OS 12.x:**
  Versionet 12.6.1 deri në 12.11.8 në modelet Firebox:
  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:**
  Versionet 2025.1 deri në 2026.1.2 në modelet Firebox:
  T115-W, T125, T125-W, T145, T145-W, T185, M295, M395, M495, M595, M695

Versionet e Korrigjuara

- **Fireware OS 12.x:** 12.12 ose më i ri
- **Fireware OS 2025.1.x:** 2026.2 ose më i ri

Rekomandime

AKSK rekomandon aplikimin e masave zbutëse ose zgjidhjeve alternative të ofruara nga WatchGuard.

Referenca

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