



AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

Dobësi me ashpërsisë të lartë në sistemin operativ WatchGuard Fireware

Data: 02/02/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive	2
Informacione Teknike	2
Rekomandime	3

Përmbledhje Ekzekutive

Një dobësi me rëndësi të lartë në WatchGuard Fireware OS të përdorur nga pajisjet Firebox mund të çojë në ekspozimin e informacionit sensitiv nga shërbimet e lidhura të autentifikimit LDAP përmes autentifikimit ose ndërfaqeve të menaxhimit të uebit

Informacione Teknike

Një dobësi me rëndësi të lartë në WatchGuard Fireware OS të përdorur nga pajisjet Firebox mund të çojë në ekspozimin e informacionit sensitiv nga shërbimet e lidhura të autentifikimit LDAP përmes autentifikimit ose ndërfaqeve të menaxhimit të uebit

Një dobësi e Injektimit LDAP me rëndësi të lartë është identifikuar në WatchGuard Fireware OS të përdorur nga pajisjet Firebox. Dobësia mund të lejojë një sulmues në distancë, të paautentifikuar, të marrë informacion sensitiv nga një server i lidhur i autentifikimit LDAP përmes autentifikimit të ekspozuar ose ndërfaqeve të menaxhimit të uebit. Në kushte të caktuara, problemi mund të aktivizojë gjithashtu autentifikimin si një përdorues LDAP duke përdorur një identifikues të pjesshëm.

Detajet e dobësisë

- CVE-2026-1498
 - Rezultati CVSS: 7.0 (I lartë)
 - Dobësia rrjedh nga validimi i pamjaftueshëm i hyrjes në trajtimin e pyetjeve LDAP brenda Fireware OS. Një sulmues i largët mund ta shfrytëzojë këtë dobësi duke injektuar pyetje të hartuara LDAP përmes ndërfaqeve të ekspozuara, duke çuar potencialisht në zbulimin e paautorizuar të informacionit të direktorisë.
- Nëse sulmuesi gjithashtu zotëron një fjalëkalim të vlefshëm të përdoruesit LDAP, identifikuesit e pjesshëm të përdoruesit mund të shfrytëzohen për të autentifikuar me sukses.

Ndikimi

Shfrytëzimi i suksesshëm mund të rezultojë në zbulim të paautorizuar të informacionit të direktorisë dhe anashkalim të mundshëm të vërtetimit, duke rritur rrezikun e kompromentimit të mëtejshëm në mjediset që mbështeten në vërtetimin e bazuar në LDAP.

Produktet e Prekura

- Fireware OS 12.0 deri në 12.11.6 duke përfshirë
- Fireware OS 2025.1 deri në 2025.1.4 duke përfshirë

Versione të përditësuar

- Fireware OS 2026.1 (për degën 2025.1)

- Fireware OS 12.11.7 (për degën 12.x)
- Fireware OS 12.5.16 (për modelin T15 dhe T35)

Rekomandime

AKSK rekomandon përditësimin e versioneve të prekura në versionet e rregulluara ose më të fundit të publikuara nga WatchGuard.