AUTORITETI KOMBËTAR
PËR SIGURINË KIBERNETIKE

Dobësi të shumta me ashpërsi të lartë në produktet Fortinet

Data: 11/03/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive 1
Informacione Teknike 1
Rekomandime 2
Referenca 2

Përmbledhje Ekzekutive

Fortinet ka publikuar disa dobësi sigurie që prekin produktet **FortiManager, FortiWeb, FortiClient Linux dhe FortiSwitch AXFixed**.

Informacione Teknike

Fortinet ka publikuar disa dobësi sigurie me nivel **të lartë** që prekin produktet **FortiManager, FortiWeb, FortiClient Linux dhe FortiSwitch AXFixed**.

1. Përshkallëzim lokal privilegjesh përmes ndjekjes së papërshtatshme të lidhjeve simbolike (symlink)

CVE ID: CVE-2026-24018
CVSS Score: 7.4
Ashpërsia: E lartë

Përshkrimi:
Një dobësi e tipit **UNIX Symbolic Link (Symlink) Following** [CWE-61] në FortiClient Linux mund të lejojë një përdorues lokal pa privilegje të përshkallëzojë privilegjet e tij deri në **root**.

Produktet e prekura dhe versionet e korrigjuara

Versioni	I prekur	Zgjidhja
FortiClient Linux 8.0	Nuk preket	Nuk aplikohet
FortiClient Linux 7.4	7.4.0 deri në 7.4.4	Përditësoni në 7.4.5 ose më të ri
FortiClient Linux 7.2	7.2.2 deri në 7.2.12	Përditësoni në 7.2.13 ose më të ri

2. Buffer Overflow përmes shërbimit fgtupdates

CVE ID: CVE-2025-54820
CVSS Score: 7.0
Ashpërsia: E lartë

Përshkrimi:
Një dobësi **Stack-based Buffer Overflow** [CWE-121] në shërbimin **fgtupdates** të FortiManager mund të lejojë një sulmues të largët pa autentikim të ekzekutojë komanda të

paautorizuara përmes kërkesave të manipuluara, nëse shërbimi është i aktivizuar. Suksesi i sulmit varet nga aftësia për të anashkaluar mekanizmat e mbrojtjes së stack-ut.

Produktet e prekura dhe versionet e korrigjuara

Versioni	I prekur	Zgjidhja
FortiManager 7.6	Nuk preket	Nuk aplikohet
FortiManager 7.4	7.4.0 deri në 7.4.2	Përditësoni në 7.4.3 ose më të ri
FortiManager 7.2	7.2.0 deri në 7.2.10	Përditësoni në 7.2.11 ose më të ri
FortiManager 6.4	Të gjitha versionet	Migrim në një version të korrigjuar

3. Anashkalim i kufizimit të përpjekjeve të autentikimit që lejon sulme brute force ndaj hyrjeve të administratorit

CVE ID: CVE-2026-24017
CVSS Score: 7.3
Ashpërsia: E lartë

Përshkrimi:
Një dobësi e tipit **Improper Control of Interaction Frequency** [CWE-799] në FortiWeb mund të lejojë një sulmues të largët pa autentikim të anashkalojë kufizimin e përpjekjeve të autentikimit përmes kërkesave të manipuluara. Suksesi i sulmit varet nga burimet e sulmuesit dhe kompleksiteti i fjalëkalimit të synuar.

Produktet e prekura dhe versionet e korrigjuara

Versioni	I prekur	Zgjidhja
FortiWeb 8.0	8.0.0 deri në 8.0.2	Përditësoni në 8.0.3 ose më të ri
FortiWeb 7.6	7.6.0 deri në 7.6.5	Përditësoni në 7.6.6 ose më të ri
FortiWeb 7.4	7.4.0 deri në 7.4.10	Përditësoni në 7.4.11 ose më të ri
FortiWeb 7.2	7.2.0 deri në 7.2.11	Përditësoni në 7.2.12 ose më të ri
FortiWeb 7.0	7.0.0 deri në 7.0.11	Përditësoni në 7.0.12 ose më të ri

Rekomandime

AKSK rekomandon të përditësoni produktet Fortinet të prekura në versionin e korrigjuar ose në versionin më të fundit të disponueshëm.

Referenca

https://fortiguard.fortinet.com/psirt/FG-IR-26-083
https://fortiguard.fortinet.com/psirt/FG-IR-25-098
https://fortiguard.fortinet.com/psirt/FG-IR-25-082
https://fortiguard.fortinet.com/psirt/FG-IR-25-086