AUTORITETI KOMBËTAR

PËR SIGURINË KIBERNETIKE

Dobësi me Rrezikshmëri të Lartë në Angular framework

Data: 18/03/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive 1
Informacione Teknike 1
Rekomandime 2
Referenca 2

Përmbledhje Ekzekutive

Është identifikuar një dobësi e rëndësishme sigurie në **Angular framework**, që prek komponentët e tij të ekzekutimit (**runtime**) dhe përpilimit (**compiler**).

Kjo dobësi lejon sulmuesit të anashkalojnë mekanizmat e integruar të sanitizimit të Angular, duke çuar potencialisht në sulme **Cross-Site Scripting (XSS)**.

Problemi lind nga trajtimi i pasaktë i atributeve të internacionalizimit (**i18n**) dhe paraqet rrezik të lartë për aplikacionet që përpunojnë input të pa besueshëm nga përdoruesit.

Informacione Teknike

Detaje të Dobësisë:

- **CVE ID:** CVE-2026-32635
- **Rrezikshmëria:** E lartë
- **CVSS:** 8.6
- Ekziston një dobësi XSS në Angular runtime dhe compiler.
- Dobësia ndodh kur një atribut i ndjeshëm për sigurinë (p.sh. **href**) shënohet për internacionalizim duke përdorur **i18n-**.
- Kjo anashkalon mekanizmat e sanitizimit të Angular dhe, kur lidhen të dhëna të pa besueshme me atributin, një sulmues mund të injektojë dhe ekzekutojë skripte keqdashëse.

Ndikimi i Mundshëm

Shfrytëzimi i suksesshëm mund të çojë në:

- rrëmbim sesioni (vjedhje e cookies dhe token-eve të autentikimit)
- nxjerrje të dhënash (akses dhe transmetim i paautorizuar i të dhënave sensitive)
- ekzekutim veprimesh të paautorizuara në emër të përdoruesve të autentikuar

Produktet e Prekura

- Aplikacionet që përdorin versione të cenueshme të Angular (runtime dhe compiler)

Versionet e Korrigjuara

- 22.0.0-next.3
- 21.2.4

- 20.3.18
- 19.2.20

Rekomandime

Rekomandohet të përditësoni versionet e prekura në versionet e korrigjuara ose në versionet më të fundit të publikuara nga Angular.

Referenca

https://www.cve.org/CVERecord?id=CVE-2026-32635