

ALVD-2026-313

ID alternative: CVE-2026-41423



8.7 | I LARTË

PËRSHKRIM

Faqet e internetit të ndërtuara me server-side rendering (SSR) të Angular-it mund të mashtrohen nga adresa interneti të krijuara posaçërisht, duke i bërë ato të dërgojnë kërkesa dhe të dhëna drejt një serveri të kontrolluar nga sulmuesi. Problemi lind kur aplikacioni pranon një kërkesë HTTP me një path që fillon me backslash (p.sh. GET /evil.com/), të cilën parser-i i URL-ve e normalizon gabimisht si forward slash. Si pasojë, aplikacioni fillon të besojë se domain-i i vet aktual është domain-i i sulmuesit. Çdo kërkesë e mëvonshme HttpClient, apo referencë të PlatformLocation.hostname, ridrejtohet automatikisht drejt serverit të huaj. Pasojat mund të përfshijnë ekspozimin e API-ve të brendshme, rrjedhjen e token-ave apo header-ave të autorizimit, dhe në infrastrukturë cloud akses potencial të shërbimet e metadata-ve. Sulmi nuk kërkon autentikim apo ndërveprim nga përdoruesi; mjafton një kërkesë e vetme e krijuar posaçërisht drejt endpoint-it SSR.

MASAT E REKOMANDUARA

Paketa @angular/platform-server duhet përditësuar në versionin e patch-uar përkatës, 19.2.21, 20.3.19, 21.2.9 ose 22.0.0-next.8, hap ky që mbetet kryesor për eliminimin e plotë të problemit. Deri në kryerjen e përditësimit, rekomandohet auditimi i kodit të aplikacionit për çdo rast kur PlatformLocation.hostname apo kërkesa HttpClient gjenerohen gjatë SSR-së pa verifikim shtesë. Kufizimi i trafikut dalës (egress) nga worker-at e SSR-së drejt shërbimeve të metadata-ve cloud (p.sh. 169.254.169.254) dhe hosteve të brendshme të ndjeshme ul ndjeshëm ndikimin e mundshëm. Vendosja e një rregulle WAF ose reverse-proxy që refuzon kërkesat HTTP me path që përmban backslash shton një shtresë shtesë mbrojtjeje.

KRITIKALITETI

CVSS Base Score:
8.7 (I lartë)
Versioni CVSS: 4.0

PUBLISHED

08.05.2026

VENDOR

Google (Angular)

PRODUCT

Angular

VERSION

17.0.0-rc.1 deri
19.2.20
20.0.0-next.0 deri
20.3.18
21.0.0-next.0 deri
21.2.8
22.0.0-next.0 deri
22.0.0-next.7

PRODUKTI I PREKUR

PRODHUESI	PRODUKTI	VERSIONI	ZGJIDHUR	PUBLIKUAR
Google (Angular)	Angular	17.0.0-rc.1 deri	19.2.21	08.05.2026
		19.2.20		
		20.0.0-next.0 deri	20.3.19	
		20.3.18		
		21.0.0-next.0 deri	21.2.9	
		21.2.8		
		22.0.0-next.0 deri	22.0.0-	
		22.0.0-next.7	next.8	

REFERENCA

- <https://github.com/angular/angular/security/advisories/GHSA-45q2-gjvg-7973>
- <https://www.cve.org/CVERecord?id=CVE-2026-41423>
- <https://euvd.enisa.europa.eu/vulnerability/CVE-2026-41423>