



Angular: SSRF via protocol-relative and backslash URLs in Angular Platform-Server

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-41423
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-08 14:16:33 UTC
Updated	2026-05-08 16:02:14 UTC
Description	Angular is a development platform for building mobile and desktop web applications using TypeScript/JavaScript and other

Risk And Classification

Primary CVSS: v4.0 8.7 HIGH from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000390000 probability, percentile 0.115560000 (date 2026-05-11)

Problem Types: CWE-918 | CWE-918 CWE-918: Server-Side Request Forgery (SSRF)

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	8.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:L/S
4.0	CNA	DECLARED	8.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:L/S

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Confidentiality

High

Integrity

None

Availability

None

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Angular	Angular	affected < 19.2.21	Not specified
CNA	Angular	Angular	affected >= 20.0.0-next.0, < 20.3.19	Not specified
CNA	Angular	Angular	affected >= 21.0.0-next.0, < 21.2.9	Not specified
CNA	Angular	Angular	affected >= 22.0.0-next.0, < 22.0.0-next.8	Not specified

References

Reference	Source	Link	Tags
github.com/angular/angular/commit/ede7c58a2aa13fdccc8f0b67ce93ba1c11749412	security-advisories@github.com	github.com	
github.com/angular/angular/security/advisories/GHSA-45q2-gjvg-7973	security-advisories@github.com	github.com	
github.com/angular/angular/pull/68194	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report