



Angular has XSS in i18n attribute bindings

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

Summary

CVE	CVE-2026-32635
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-16 14:19:40 UTC
Updated	2026-04-30 18:23:13 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 8.6 HIGH from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/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

Problem Types: CWE-79 | CWE-79 CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	8.6	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:H/VI:H/VA:H/SC:N
4.0	CNA	DECLARED	8.6	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:H/VI:H/VA:H/SC:N
3.1	nvd@nist.gov	Primary	9	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/H:I/H:A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

Passive

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Angular	Angular Cli	All	All	All	All
Application	Angular	Angular Cli	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	@angular	Compiler	affected >= 22.0.0-next.0, < 22.0.0-next.3	Not specified

CNA	@angular	Compiler	affected >= 21.0.0-next.0, < 21.2.4	Not specified
CNA	@angular	Compiler	affected >= 20.0.0-next.0, < 20.3.18	Not specified
CNA	@angular	Compiler	affected >= 17.0.0.next.0, < 19.2.20	Not specified
CNA	@angular	Core	affected >= 22.0.0-next.0, < 22.0.0-next.3	Not specified
CNA	@angular	Core	affected >= 21.0.0-next.0, < 21.2.4	Not specified
CNA	@angular	Core	affected >= 20.0.0-next.0, < 20.3.18	Not specified
CNA	@angular	Core	affected >= 17.0.0.next.0, < 19.2.20	Not specified

References

Reference	Source	Link	Tags
github.com/angular/angular/pull/67541	security-advisories@github.com	github.com	Issue Tracking, P
github.com/angular/angular/security/advisories/GHSA-g93w-mfhg-p222	security-advisories@github.com	github.com	Vendor Advisory,
github.com/angular/angular/pull/67561	security-advisories@github.com	github.com	Issue Tracking, P
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analys

No vendor comments have been submitted for this CVE.

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

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#)