



webpack-dev-server vulnerable to cross-origin source code exposure on non-HTTPS origins

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

Summary

CVE	CVE-2026-6402
State	PUBLISHED
Assigner	openjs
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-12 09:16:55 UTC
Updated	2026-05-12 09:16:55 UTC
Description	webpack-dev-server versions up to and including 5.2.3 are vulnerable to cross-origin source code exposure when serving o

Risk And Classification

Primary CVSS: v3.1 5.3 MEDIUM from ce714d77-add3-4f53-aff5-83d477b104bb

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

Problem Types: CWE-749 | CWE-749 CWE-749: Exposed Dangerous Method or Function

Version	Source	Type	Score	Severity	Vector
3.1	ce714d77-add3-4f53-aff5-83d477b104bb	Secondary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N
3.1	CNA	CVSS	5.3	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Webpack-dev-server	Webpack-dev-server	affected 5.2.4 semver	Not specified
CNA	Webpack-dev-server	Webpack-dev-server	unaffected 5.2.4 semver	Not specified

References

Reference	Source	Link
cna.openjsf.org/security-advisories.html	ce714d77-add3-4f53-aff5-83d477b104bb	cna.openjsf.org
github.com/webpack/webpack-dev-server/security/advisories/GHSA-79cf-xcqc...	ce714d77-add3-4f53-aff5-83d477b104bb	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: [sapphi-red \(en\)](#)

CNA: [Ulises Gascón \(en\)](#)

CNA: [Sebastian Beltran \(en\)](#)

CNA: [Alexander Akait \(en\)](#)

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