



# CVE-2026-1615

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2026-1615
<b>State</b>	PUBLISHED
<b>Assigner</b>	snyk
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-02-09 05:16:24 UTC
<b>Updated</b>	2026-04-29 01:00:01 UTC
<b>Description</b>	Versions of the package jsonpath before 1.3.0 are vulnerable to Arbitrary Code Injection via unsafe evaluation of user-sup

## Risk And Classification

**Primary CVSS:** v4.0 8.2 HIGH from report@snyk.io

**CVSS:**4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P/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:** 0.001030000 probability, percentile 0.280950000 (date 2026-04-07)

**Problem Types:** CWE-94 | CWE-94 Arbitrary Code Injection

Version	Source	Type	Score	Severity	Vector
4.0	report@snyk.io	Secondary	8.2	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P/C.
4.0	CNA	DECLARED	9.2	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P
3.1	report@snyk.io	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSG:X/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

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	Jsonpath	affected 1.3.0 semver	Not specified
CNA	Na	Org.webjars.npmjsonpath	affected * semver	Not specified

### References

Reference	Source	Link	Type
-----------	--------	------	------

Reference	Source	Link	Tags
security.snyk.io/vuln/SNYK-JS-JSONPATH-13645034	report@snyk.io	<a href="https://security.snyk.io">security.snyk.io</a>	
github.com/dchester/jsonpath/commit/b61111f07ac1a8d0f3133b5fc51438ecb76a...	report@snyk.io	<a href="https://github.com">github.com</a>	
security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-15141219	report@snyk.io	<a href="https://security.snyk.io">security.snyk.io</a>	
github.com/dchester/jsonpath/blob/c1dd8ec74034fb0375233abb5fdbec51ac317b...	report@snyk.io	<a href="https://github.com">github.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

### Vendor Comments And Credit

#### Discovery Credit

**CNA:** Nick Copi (en)

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)