



# CVE-2026-3884

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

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2026-3884   |
| <b>State</b>           | PUBLISHED   |
| <b>Assigner</b>        | snyk  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2026-03-11 06:17:15 UTC   |
| <b>Updated</b>         | 2026-05-07 18:08:05 UTC   |
| <b>Description</b>     | Versions of the package spin.js before 3.0.0 are vulnerable to Cross-site Scripting (XSS) via the spin() function that allows c |

## Risk And Classification

**Primary CVSS:** v4.0 2 LOW from report@snyk.io

**CVSS:**4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/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:** 0.000340000 probability, percentile 0.101340000 (date 2026-05-11)

**Problem Types:** CWE-79 | CWE-79 Cross-site Scripting (XSS)

| Version | Source         | Type      | Score | Severity | Vector   |
|---------|----------------|-----------|-------|----------|--|
| 4.0     | report@snyk.io | Secondary | 2     | LOW      | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N/E:P/C... |
| 4.0     | CNA            | DECLARED  | 5.1   | MEDIUM   | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N/E:P      |
| 3.1     | report@snyk.io | Secondary | 6.1   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N                             |
| 3.1     | CNA            | DECLARED  | 6.1   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P                         |

## CVSS v4.0 Breakdown

Attack Vector

**Network**

Attack Complexity

**Low**

Attack Requirements

**None**

Privileges Required

**None**

User Interaction

**None**

Active

Confidentiality

None

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:A/VC:N/VI:N/VA:N/SC:L/SI:L/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

### CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

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

### NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor  | Product | Version | Update | Edition | Language |
|-------------|---------|---------|---------|--------|---------|----------|
| Application | Spin.js | Spin.js | All     | All    | All     | All      |

### Vendor Declared Affected Products

| Source | Vendor  | Product | Version               | Platforms     |
|--------|---------|---------|-----------------------|---------------|
| CNA    | Spin.js | Spin.js | affected 2.0.0 com... | Not specified |

CNA      na      spin.js      affected 3.0.0 semver      not specified

## References

| Reference   | Source         | Link  | Tags                 |
|---|----------------|---|----------------------|
| <a href="https://security.snyk.io/vuln/SNYK-JS-SPINJS-15445079">security.snyk.io/vuln/SNYK-JS-SPINJS-15445079</a>                                       | report@snyk.io | <a href="https://security.snyk.io">security.snyk.io</a> | Third Party Advisory |
| <a href="https://gist.github.com/ericcornelissen/1a73e28fa50c3009b0eb51ad2fc19f25">gist.github.com/ericcornelissen/1a73e28fa50c3009b0eb51ad2fc19f25</a> | report@snyk.io | <a href="https://gist.github.com">gist.github.com</a>   | Broken Link          |
| 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:** Eric Cornelissen (en)

**CNA:** Samuel Kajava (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](https://cve.report/api)

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