



# WordPress WP Social Widget plugin <= 2.2.5 - Cross Site Scripting (XSS) vulnerability

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

## Summary

|                        |                                                                                                                             |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2024-27189                                                                                                              |
| <b>State</b>           | PUBLISHED                                                                                                                   |
| <b>Assigner</b>        | Patchstack                                                                                                                  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                |
| <b>Published</b>       | 2024-03-15 13:15:08 UTC                                                                                                     |
| <b>Updated</b>         | 2026-04-28 19:23:33 UTC                                                                                                     |
| <b>Description</b>     | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in catchsquare WP Social |

## Risk And Classification

**Primary CVSS:** v3.1 5.4 MEDIUM from nvd@nist.gov

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

**EPSS:** 0.000770000 probability, percentile 0.228270000 (date 2026-04-28)

**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                                       |
|---------|----------------------|-----------|-------|----------|----------------------------------------------|
| 3.1     | nvd@nist.gov         | Primary   | 5.4   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N |
| 3.1     | audit@patchstack.com | Secondary | 6.5   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L |
| 3.1     | CNA                  | CVSS      | 6.5   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L |

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:L/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 | Catchsquare | Wp Social Widget | All     | All    | All     | All      |

Vendor Declared Affected Products

| Source | Vendor      | Product          | Version                   | Platforms     |
|--------|-------------|------------------|---------------------------|---------------|
| CNA    | Catchsquare | WP Social Widget | affected n/a 2.2.5 custom | Not specified |

References

| Reference                                                                                          | Source                            |
|----------------------------------------------------------------------------------------------------|-----------------------------------|
| WordPress WP Social Widget plugin <= 2.2.5 - Cross Site Scripting (XSS) vulnerability - Patchstack | af854a3a-2127-422b-91ae-364da2661 |
| CVE Program record                                                                                 | CVE.ORG                           |
| NVD vulnerability detail                                                                           | NVD                               |

Vendor Comments And Credit

Discovery Credit

CNA: LVT-tholv2k (Patchstack Alliance) (en)

Additional Advisory Data

Solutions

CNA: Update to 2.2.6 or a higher version.

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](https://cve.report/api)

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