



# WordPress Tapfiliate plugin <= 3.2.2 - Cross Site Scripting (XSS) vulnerability

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

| Summary         |                                                                                                                                  |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2025-58689                                                                                                                   |
| State           | PUBLISHED                                                                                                                        |
| Assigner        | Patchstack                                                                                                                       |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                     |
| Published       | 2025-09-22 19:16:20 UTC                                                                                                          |
| Updated         | 2026-04-23 15:33:36 UTC                                                                                                          |
| Description     | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tapfiliate Tapfiliate tapf |

Risk And Classification

Primary CVSS: v3.1 6.5 MEDIUM from audit@patchstack.com

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

EPSS: 0.000360000 probability, percentile 0.106600000 (date 2026-04-23)

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

| Version | Source               | Type      | Score | Severity | Vector                                       |
|---------|----------------------|-----------|-------|----------|----------------------------------------------|
| 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

Low

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

Vendor Declared Affected Products

| Source | Vendor     | Product    | Version               | Platforms     |
|--------|------------|------------|-----------------------|---------------|
| CNA    | Tapfiliate | Tapfiliate | affected 3.2.2 custom | Not specified |

References

| Reference                                                                       | Source               | Link           | Tags             |
|---------------------------------------------------------------------------------|----------------------|----------------|------------------|
| patchstack.com/database/Wordpress/Plugin/tapfiliate/vulnerability/wordpress-... | audit@patchstack.com | patchstack.com |                  |
| CVE Program record                                                              | CVE.ORG              | www.cve.org    | canonical        |
| NVD vulnerability detail                                                        | NVD                  | nvd.nist.gov   | canonical, analy |

Vendor Comments And Credit

Discovery Credit

CNA: Gilang Asra Bilhadi - DJ | Patchstack Bug Bounty Program (en)

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