



WordPress Click & Tweet Plugin <= 0.8.9 - Cross Site Scripting (XSS) Vulnerability

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary

CVE	CVE-2025-60179
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-09-26 09:15:47 UTC
Updated	2026-04-28 19:34:40 UTC
Description	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Space Studio Click & T

Risk And Classification

Primary CVSS: v3.1 5.9 MEDIUM from audit@patchstack.com

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

EPSS: 0.000290000 probability, percentile 0.080800000 (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	audit@patchstack.com	Secondary	5.9	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:L
3.1	CNA	CVSS	5.9	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

Low

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Space Studio	Click Tweet	affected n/a 0.8.9 custom	Not specified

References

Reference

[patchstack.com/database/wordpress/plugin/click-tweet/vulnerability/wordpress...](#)

<https://patchstack.com/database/wordpress/plugin/click-tweet/vulnerability/wordpress-click-tweet-plugin-0-8-9-cross-site-scripting-xss-vulnerak>

CVE Program record

NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

CNA: Nabil Irawan (Patchstack Alliance) (en)

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