# WordPress Click To Tweet plugin <= 2.0.14 - Broken Access Control vulnerability

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2023-41857 |
| **State** | PUBLISHED |
| **Assigner** | Patchstack |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2024-12-13 15:15:24 UTC |
| **Updated** | 2026-04-28 19:21:20 UTC |
| **Description** | Missing Authorization vulnerability in ClickToTweet.com Click To Tweet allows Exploiting Incorrectly Configured Access Co |

## Risk And Classification

**Primary CVSS:** v3.1 5.4 MEDIUM from audit@patchstack.com

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

**EPSS:** 0.001640000 probability, percentile 0.369450000 (date 2026-05-14)

**Problem Types:** CWE-862 | CWE-862 CWE-862 Missing Authorization

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 3.1 | audit@patchstack.com | Secondary | 5.4 | MEDIUM | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L |
| 3.1 | CNA | CVSS | 5.4 | MEDIUM | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L |

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

ntegrity

Low

Availability

Low

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

## Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|---|---|---|---|---|
| CNA | ClickToTweet.com | Click To Tweet | affected n/a 2.0.14 custom | Not specified |

## References

| Reference |
|---|
| patchstack.com/database/wordpress/plugin/click-to-tweet/vulnerability/wordpr... |
| https://patchstack.com/database/wordpress/plugin/click-to-tweet/vulnerability/wordpress-click-to-tweet-plugin-2-0-14-broken-access-control-vu |
| CVE Program record |
| NVD vulnerability detail |

## Vendor Comments And Credit

Discovery Credit

**CNA:** thiennv (Patchstack Alliance) (en)

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