# CVE-2014-2559

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2014-2559 |
| **State** | PUBLISHED |
| **Assigner** | mitre |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2014-10-17 22:55:04 UTC |
| **Updated** | 2026-05-06 22:30:45 UTC |
| **Description** | Multiple cross-site request forgery (CSRF) vulnerabilities in twitget.php in the Twitget plugin before 3.3.3 for WordPress allo |

## Risk And Classification

**Primary CVSS:** v2.0 6.8 from nvd@nist.gov

AV:N/AC:M/Au:N/C:P/I:P/A:P

**Problem Types:** CWE-352 | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:M/Au:N/C:P/I:P/A:P

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Twitget Project | Twitget | All | All | All | All |

## Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|---|---|---|---|---|
| CNA | Na | N/a | affected n/a | Not specified |

## References

| Reference | Source |
|---|---|
| CSRF/XSS vulnerability in Twitget 3.3.1 – dxw advisories | af854a3a-2127-422b-91ae-364 |
| Security Advisory SA57892 - WordPress Twitget Plugin Cross-Site Request Forgery Vulnerability - Secunia | af854a3a-2127-422b-91ae-364 |
| Twitget 3.3.1 Cross Site Request Forgery / Cross Site Scripting ≈ Packet Storm | af854a3a-2127-422b-91ae-364 |
| WordPress › Twitget « WordPress Plugins | af854a3a-2127-422b-91ae-364 |
| Full Disclosure: CSRF/XSS vulnerability in Twitget 3.3.1 (WordPress plugin) | af854a3a-2127-422b-91ae-364 |
| IBM X-Force Exchange | af854a3a-2127-422b-91ae-364 |
| CVE Program record | CVE.ORG |
| NVD vulnerability detail | NVD |

No vendor comments have been submitted for this CVE.

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