# WordPress WPShapere Lite plugin <= 1.4.1 - Cross Site Request Forgery (CSRF) Vulnerability

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2025-53317 |
| **State** | PUBLISHED |
| **Assigner** | Patchstack |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2025-06-27 14:15:54 UTC |
| **Updated** | 2026-04-23 15:32:29 UTC |
| **Description** | Cross-Site Request Forgery (CSRF) vulnerability in AcmeeDesign WPShapere - WordPress admin theme wpshapere-lite a |

## Risk And Classification

**Primary CVSS:** v3.1 7.1 HIGH from audit@patchstack.com

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

**Problem Types:** CWE-352 | CWE-352 Cross-Site Request Forgery (CSRF)

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 3.1 | audit@patchstack.com | Secondary | 7.1 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L |
| 3.1 | CNA | CVSS | 7.1 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L |

### CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
Low

Privileges Required
None

User Interaction
Required

Scope
Changed

Confidentiality
Low

Integrity
Low

Availability

Low

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

## Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|---|---|---|---|---|
| CNA | AcmeeDesign | WPShapere - WordPress Admin Theme | affected 1.4.1 custom | Not specified |

## References

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

## Vendor Comments And Credit

Discovery Credit

**CNA:** Skalucy | Patchstack Bug Bounty Program (en)

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