



# WordPress WZone plugin <= 14.0.10 - Reflected Cross Site Scripting (XSS) vulnerability

[MITRE](#)

[NVD](#)

[CVE.ORG](#)

[JSON API](#)

[Print: PDF](#)

## Summary

|                 |                                                                                                                           |
|-----------------|---------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2024-33548                                                                                                            |
| State           | PUBLISHED                                                                                                                 |
| Assigner        | Patchstack                                                                                                                |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                              |
| Published       | 2024-04-29 06:15:10 UTC                                                                                                   |
| Updated         | 2026-04-28 19:25:05 UTC                                                                                                   |
| Description     | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AA-Team WZone allow |

## 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

**EPSS:** 0.001970000 probability, percentile 0.414480000 (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 | 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    | AA-Team | WZone   | affected n/a 14.0.10 custom | Not specified |

References

| Reference                                                                       | Source                               | Link        |
|---------------------------------------------------------------------------------|--------------------------------------|-------------|
| patchstack.com/database/vulnerability/woozone/wordpress-wzone-plugin-14-0-10... | af854a3a-2127-422b-91ae-364da2661108 | patchstack  |
| CVE Program record                                                              | CVE.ORG                              | www.cve.c   |
| NVD vulnerability detail                                                        | NVD                                  | nvd.nist.gc |

Vendor Comments And Credit

Discovery Credit

CNA: Rafie Muhammad (Patchstack) (en)

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