



# WordPress Interactive World Map plugin <= 3.4.4 - Cross Site Scripting (XSS) vulnerability

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

| Summary         |                                                                                                                             |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2024-50462                                                                                                              |
| State           | PUBLISHED                                                                                                                   |
| Assigner        | Patchstack                                                                                                                  |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                |
| Published       | 2024-10-28 18:15:07 UTC                                                                                                     |
| Updated         | 2026-04-23 15:19:59 UTC                                                                                                     |
| Description     | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in html5maps Interactive |

Risk And Classification

Primary CVSS: v3.1 6.5 MEDIUM from audit@patchstack.com

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

Problem Types: 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 | 6.5   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L |
| 3.1     | CNA                  | CVSS      | 6.5   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L |

| CVSS v3.1 Breakdown |          |
|---------------------|----------|
| Attack Vector       | Network  |
| Attack Complexity   | Low      |
| Privileges Required | Low      |
| User Interaction    | Required |
| Scope               | Changed  |
| Confidentiality     | Low      |
| Integrity           |          |

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

Vendor Declared Affected Products

| Source | Vendor    | Product               | Version               | Platforms     |
|--------|-----------|-----------------------|-----------------------|---------------|
| CNA    | Html5maps | Interactive World Map | affected 3.4.4 custom | Not specified |

References

| Reference                                                                       | Source               | Link           | Tags           |
|---------------------------------------------------------------------------------|----------------------|----------------|----------------|
| patchstack.com/database/Wordpress/Plugin/interactive-world-map/vulnerability... | 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: Sc1duck | Patchstack Bug Bounty Program (en)

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