



# WordPress YaMaps for WordPress plugin <= 0.6.40 - Cross Site Scripting (XSS) vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |                                                                                                                           |
|------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2025-32172                                                                                                            |
| <b>State</b>           | PUBLISHED                                                                                                                 |
| <b>Assigner</b>        | Patchstack                                                                                                                |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                              |
| <b>Published</b>       | 2025-04-04 16:15:26 UTC                                                                                                   |
| <b>Updated</b>         | 2026-04-23 15:28:41 UTC                                                                                                   |
| <b>Description</b>     | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Yuri Baranov YaMaps |

## 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    | Yuri Baranov | YaMaps For WordPress | affected 0.6.40 custom | Not specified |

References

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

Vendor Comments And Credit

Discovery Credit

CNA: Peter Thaleikis | Patchstack Bug Bounty Program (en)

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