



# WordPress WP Photo Sphere plugin <= 3.8 - Cross Site Scripting (XSS) vulnerability

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

## Summary

<b>CVE</b>	CVE-2025-23924
<b>State</b>	PUBLISHED
<b>Assigner</b>	Patchstack
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-01-16 21:15:34 UTC
<b>Updated</b>	2026-04-23 15:24:47 UTC
<b>Description</b>	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jeremy WP Photo Sph

## 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

Low

Availability

Low

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	Jeremy	WP Photo Sphere	affected 3.8 custom	Not specified

### References

Reference	Source	Link	Tags
patchstack.com/database/Wordpress/Plugin/wp-photo-sphere/vulnerability/wordp...	audit@patchstack.com	<a href="https://patchstack.com">patchstack.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, a

### 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.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)