



# WordPress Move Addons for Elementor plugin <= 1.3.4 - Cross Site Scripting (XSS) vulnerability

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

## Summary

<b>CVE</b>	CVE-2024-47364
<b>State</b>	PUBLISHED
<b>Assigner</b>	Patchstack
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-10-06 10:15:05 UTC
<b>Updated</b>	2026-04-23 15:19:14 UTC
<b>Description</b>	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in moveaddons Move Ad

## Risk And Classification

**Primary CVSS:** v3.1 5.4 MEDIUM from nvd@nist.gov

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

**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	nvd@nist.gov	Primary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N
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  
 None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Moveaddons</a>	<a href="#">Move Addons For Elementor</a>	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Moveaddons</a>	<a href="#">Move Addons For Elementor</a>	affected 1.3.4 custom	Not specified

References

Reference	Source	Link	Tags
<a href="#">patchstack.com/database/Wordpress/Plugin/move-addons/vulnerability/wordpress...</a>	<a href="mailto:audit@patchstack.com">audit@patchstack.com</a>	<a href="#">patchstack.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, s

Vendor Comments And Credit

Discovery Credit  
**CNA: João Pedro S Alcântara (Kinorth) | Patchstack Bug Bounty Program (en)**

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