



# WordPress WP Log Action Plugin <= 0.51 - Reflected Cross Site Scripting (XSS) vulnerability

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

## Summary

<b>CVE</b>	CVE-2025-24619
<b>State</b>	PUBLISHED
<b>Assigner</b>	Patchstack
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-04-17 16:15:32 UTC
<b>Updated</b>	2026-04-23 15:25:08 UTC
<b>Description</b>	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in webheadcoder WP Log

## 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

**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	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

