WPC Composite Products for WooCommerce <= 7.2.7 - Authenticated (Subscriber+) Stored Cross-Site Scripting

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2024-2838
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-04-27 04:15:09 UTC
Updated	2026-04-08 19:21:12 UTC
Description	The WPC Composite Products for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the

Risk And Classification

Primary CVSS: v3.1 6.4 MEDIUM from security@wordfence.com

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

EPSS: 0.001830000 probability, percentile 0.400830000 (date 2026-04-12)

Problem Types: CWE-79 | CWE-79 CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	6.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
3.1	CNA	DECLARED	6.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Wpclever	WPC Composite Products For WooCommerce	affected 7.2.7 semver	Not specified
ADP	Wpclever	Wpc Product Bundles For Woocommerce	affected 7.2.7 semver	Not specified

References

Reference	Source
www.wordfence.com/threat-intel/vulnerabilities/id/d3bea017-9fc3-4e14-97c4-5bb52...	af854a3a-2127-422b-91ae-364da2661108
plugins.trac.wordpress.org/changeset/3069973/wpc-composite-products/trunk/includes/class...	af854a3a-2127-422b-91ae-364da2661108
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

CNA: Krzysztof Zając (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-04-26T00:00:00.000Z	Disclosed

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

CVE.report and Source URL Uptime Status status.cve.report