WordPress WooCommerce Payments Plugin <= 6.4.2 is vulnerable to Cross Site Scripting (XSS)

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

Summary

CVE	CVE-2023-49828
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-12-14 15:15:09 UTC
Updated	2026-04-28 19:22:27 UTC
Description	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Automattic WooPayme

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

EPSS: 0.001550000 probability, percentile 0.359250000 (date 2026-04-28)

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	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	Automattic	Woopayments	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Automattic	WooPayments Fully Integrated Solution Built And Supported By Woo	affected n/a 6.4.2 custom	Not specified

References

Reference	Source	Link
patchstack.com/database/vulnerability/woocommerce-payments/wordpress-woopaym...	af854a3a-2127-422b-91ae-364da2661108	patchs
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.ni

Vendor Comments And Credit

Discovery Credit

CNA: Rafie Muhammad (Patchstack) (en)

Additional Advisory Data

Solutions

CNA: Update to 6.5.0 or a higher version.

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

Free CVE JSON API cve.report/api

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