PeproDev WooCommerce Receipt Uploader <= 2.6.9 - Reflected Cross-Site Scripting

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

Summary

CVE	CVE-2024-8873
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-11-16 04:15:06 UTC
Updated	2026-04-08 19:22:31 UTC
Description	The PeproDev WooCommerce Receipt Uploader plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due t

Risk And Classification

Primary CVSS: v3.1 6.1 MEDIUM from security@wordfence.com

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

EPSS: 0.030430000 probability, percentile 0.866800000 (date 2026-04-13)

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	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
3.1	CNA	DECLARED	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

ntegrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Peprodev	PeproDev WooCommerce Receipt Uploader	affected 2.6.9 semver	Not specified

References

Reference	Source	Link
www.wordfence.com/threat-intel/vulnerabilities/id/e09c2916-6e2c-4db3-901a-b5715...	security@wordfence.com	www.wordfenc
plugins.trac.wordpress.org/changeset/3194699/pepro-bacs-receipt-upload-for-woocommerce/t...	security@wordfence.com	plugins.trac.wo
plugins.trac.wordpress.org/browser/pepro-bacs-receipt-upload-for-woocommerce/trunk/wc-up...	security@wordfence.com	plugins.trac.wo
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: vgo0 (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-11-15T15:15:29.000Z	Disclosed

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