Parcel Pro <= 1.8.4 - Reflected Cross-Site Scripting

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

Summary

CVE	CVE-2024-9383
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-10-18 05:15:07 UTC
Updated	2026-04-08 18:22:53 UTC
Description	The Parcel Pro plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'action' parameter in all versions

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: 0.025660000 probability, percentile 0.856960000 (date 2026-05-18)

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Parcelpro	Parcel Pro	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Parcelpro	Parcel Pro	affected 1.8.4 semver	Not specified

References

Reference	Source	Link
www.wordfence.com/threat-intel/vulnerabilities/id/8e8fe6f4-7e41-44d3-9980-b5e7f...	security@wordfence.com	www.wordfence.c
plugins.trac.wordpress.org/browser/woo-parcel-pro/trunk/admin/class-parcelpro-admin.php	security@wordfence.com	plugins.trac.word
plugins.trac.wordpress.org/changeset/3174370/woo-parcel-pro/trunk/admin/class-parcelpro-...	security@wordfence.com	plugins.trac.word
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	2024-10-17T15:42:33.000Z	Disclosed

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

site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

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