WordPress WP AVCL Automation Helper (formerly WPFlyLeads) plugin <= 3.4 - Server Side Request Forgery (SSRF) Vulnerability

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

Summary

CVE	CVE-2025-46531
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-04-24 16:15:44 UTC
Updated	2026-04-23 15:30:11 UTC
Description	Server-Side Request Forgery (SSRF) vulnerability in Ankur Vishwakarma WP AVCL Automation Helper (formerly WPFlyLe

Risk And Classification

Primary CVSS: v3.1 4.9 MEDIUM from audit@patchstack.com

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

Problem Types: CWE-918 | CWE-918 Server-Side Request Forgery (SSRF)

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	4.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:N
3.1	CNA	CVSS	4.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

Low

ntegrity

Low

vailability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Ankur Vishwakarma	WP AVCL Automation Helper Formerly WPFlyLeads	affected 3.4 custom	Not specified

References

Reference	Source	Link	Tags
patchstack.com/database/Wordpress/Plugin/woozap/vulnerability/wordpress-wp-a...	audit@patchstack.com	patchstack.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

Vendor Comments And Credit

Discovery Credit

CNA: ch4r0n | Patchstack Bug Bounty Program (en)

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