WordPress MoveTo Plugin <= 6.2 is vulnerable to Arbitrary File Upload

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

Summary

CVE	CVE-2024-25913
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-02-26 16:27:59 UTC
Updated	2026-04-28 19:23:30 UTC
Description	Unrestricted Upload of File with Dangerous Type vulnerability in Skymoonlabs MoveTo.This issue affects MoveTo: from n/a

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from nvd@nist.gov

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

EPSS: 0.007710000 probability, percentile 0.736190000 (date 2026-04-28)

Problem Types: CWE-434 | CWE-434 CWE-434 Unrestricted Upload of File with Dangerous Type

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	audit@patchstack.com	Secondary	10	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	CVSS	10	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Skymoonlabs	Moveto	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Skymoonlabs	MoveTo	affected n/a 6.2 custom	Not specified
ADP	Skymoonlabs	Moveto	affected 6.2 custom	Not specified

References

Reference	Source	Link
patchstack.com/database/vulnerability/moveto/wordpress-moveto-plugin-6-2-una...	af854a3a-2127-422b-91ae-364da2661108	patchstack.
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

Vendor Comments And Credit

Discovery Credit

CNA: Dave Jong (Patchstack) (en)

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