



WordPress Post/Page Copying Tool plugin <= 2.0.0 - Sensitive Data Exposure vulnerability

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary	
CVE	CVE-2024-56300
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-01-07 11:15:13 UTC
Updated	2026-04-23 15:22:51 UTC
Description	Insertion of Sensitive Information Into Sent Data vulnerability in wpspin Post/Page Copying Tool postpage-import-export-wi

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from audit@patchstack.com

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

Problem Types: CWE-201 | CWE-201 Insertion of Sensitive Information Into Sent Data

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	CNA	CVSS	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v3.1 Breakdown	
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	None

Availability

None

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



Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Wpspin	Post/Page Copying Tool	affected 2.0.0 custom	Not specified

References

Reference	Source	Link	Tags
patchstack.com/database/Wordpress/Plugin/postpage-import-export-with-custom-...	audit@patchstack.com	patchstack.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, &



Vendor Comments And Credit

Discovery Credit

CNA: stealthcopter | Patchstack Bug Bounty Program (en)

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