

WordPress Zero Spam for WordPress plugin <= 5.5.6 - Bypass Spam Protection vulnerability

MITRE

NVD

CVE.ORG

JSON API

Print: PDF 

Summary	
CVE	CVE-2024-32521
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-05-17 09:15:37 UTC
Updated	2026-04-28 19:24:43 UTC
Description	Client-Side Enforcement of Server-Side Security vulnerability in Highfivory LLC Zero Spam allows Removing Important Clie

Risk And Classification

Primary CVSS: v3.1 5.3 MEDIUM from audit@patchstack.com

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

EPSS: 0.006740000 probability, percentile 0.714760000 (date 2026-04-28)

Problem Types: CWE-602 | CWE-602 CWE-602 Client-Side Enforcement of Server-Side Security

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
3.1	CNA	CVSS	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

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

None

Integrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Highfivery LLC	Zero Spam	affected n/a 5.5.6 custom	Not specified
ADP	Highfivery	Zero Spam For Wordpress	affected 5.5.6 custom	Not specified

References

Reference	Source	Link
patchstack.com/database/vulnerability/zero-spam/wordpress-zero-spam-for-word...	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: Brandon Roldan (Patchstack Alliance) (en)

Additional Advisory Data

Solutions

CNA: Update to 5.5.7 or a higher version.

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