



WordPress Spider Elements – Addons for Elementor plugin <= 1.6.6 - Broken Access Control vulnerability

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary	
CVE	CVE-2025-32216
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-04-10 08:15:18 UTC
Updated	2026-04-23 15:28:46 UTC
Description	Missing Authorization vulnerability in Spider Themes Spider Elements spider-elements allows Exploiting Incorrectly Configu

Risk And Classification					
Primary CVSS: v3.1 6.4 MEDIUM from audit@patchstack.com					
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:L/A:L					
Problem Types: CWE-862 CWE-862 Missing Authorization					
Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	6.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:L/A:L
3.1	CNA	CVSS	6.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:L/A:L

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

Availability

Low

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



Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Spider Themes	Spider Elements	affected 1.6.6 custom	Not specified

References

Reference	Source	Link	Tags
patchstack.com/database/Wordpress/Plugin/spider-elements/vulnerability/wordp...	audit@patchstack.com	patchstack.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, an



Vendor Comments And Credit

Discovery Credit

CNA: Abu Hurayra | Patchstack Bug Bounty Program (en)

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