



WordPress BBP Core plugin <= 1.4.1 - Broken Access Control vulnerability

[MITRE](#)

[NVD](#)

[CVE.ORG](#)

[JSON API](#)

[Print: PDF](#)

Summary

CVE	CVE-2025-68572
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-12-24 13:16:24 UTC
Updated	2026-04-27 19:16:31 UTC
Description	Missing Authorization vulnerability in Spider Themes BBP Core bbp-core allows Exploiting Incorrectly Configured Access C

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: 0.000560000 probability, percentile 0.172850000 (date 2026-04-27)

Problem Types: CWE-862 | CWE-862 Missing Authorization

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

ntegrity

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	Spider Themes	BBP Core	affected 1.4.1 custom	Not specified

References

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

Vendor Comments And Credit

Discovery Credit

CNA: daroo | Patchstack Bug Bounty Program (en)

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