



WordPress Advanced Post List plugin <= 0.5.6.2 - Cross Site Request Forgery (CSRF) Vulnerability

[MITRE](#)

[NVD](#)

[CVE.ORG](#)

[JSON API](#)

[Print: PDF](#)

Summary	
CVE	CVE-2025-30968
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-06-06 13:15:37 UTC
Updated	2026-04-23 15:27:25 UTC
Description	Cross-Site Request Forgery (CSRF) vulnerability in jokerbr313 Advanced Post List advanced-post-list allows Cross Site Re

Risk And Classification

Primary CVSS: v3.1 5.4 MEDIUM from audit@patchstack.com

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

Problem Types: CWE-352 | CWE-352 Cross-Site Request Forgery (CSRF)

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L
3.1	CNA	CVSS	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

Low

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



Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Jokerbr313	Advanced Post List	affected 0.5.6.2 custom	Not specified

References

Reference	Source	Link	Tags
patchstack.com/database/Wordpress/Plugin/advanced-post-list/vulnerability/wo...	audit@patchstack.com	patchstack.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana



Vendor Comments And Credit

Discovery Credit

CNA: Nguyen Xuan Chien | Patchstack Bug Bounty Program (en)

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