WordPress Advanced Access Manager Plugin <= 6.9.18 is vulnerable to Open Redirection

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2023-51675
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-12-29 14:15:48 UTC
Updated	2026-04-28 19:22:54 UTC
Description	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in AAM Advanced Access Manager – Restricted Content,

Risk And Classification

Primary CVSS: v3.1 5.4 MEDIUM from nvd@nist.gov

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

EPSS: 0.001890000 probability, percentile 0.404990000 (date 2026-04-28)

Problem Types: CWE-601 | CWE-601 CWE-601 URL Redirection to Untrusted Site ('Open Redirect')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N
3.1	audit@patchstack.com	Secondary	4.7	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:N/A:N
3.1	CNA	CVSS	4.7	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vasyltech	Advanced Access Manager	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	AAM	Advanced Access Manager Restricted Content Users Roles Enhanced Security And More	affected n/a 6.9.18 custom

References

Reference	Source	Link
patchstack.com/database/vulnerability/advanced-access-manager/wordpress-adva...	af854a3a-2127-422b-91ae-364da2661108	patchstac
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

Vendor Comments And Credit

Discovery Credit

CNA: LVT-tholv2k (Patchstack Alliance) (en)

Additional Advisory Data

Solutions

CNA: Update to 6.9.19 or a higher version.

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

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report