



WordPress ARMember – Membership Plugin plugin <= 4.0.28 - Broken Access Control vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2024-32948
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-04-24 07:15:48 UTC
Updated	2026-04-28 19:25:01 UTC
Description	Missing Authorization vulnerability in Repute Infosystems ARMember. This issue affects ARMember: from n/a through 4.0.2

Risk And Classification

Primary CVSS: v3.1 9.1 CRITICAL from audit@patchstack.com

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

EPSS: 0.001430000 probability, percentile 0.342410000 (date 2026-04-28)

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

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H
3.1	CNA	CVSS	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Reputeinfosystems	Armember	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Repute Infosystems	ARMember	affected n/a 4.0.28 custom	Not specified
ADP	Armemberplugin	Armember	affected 4.0.28 semver	Not specified

References

Reference	Source	Link
patchstack.com/database/vulnerability/armmember-membership/wordpress-armmember-...	af854a3a-2127-422b-91ae-364da2661108	patchst
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

Vendor Comments And Credit

Discovery Credit

CNA: Kursat Cetin (Patchstack) (en)

Additional Advisory Data

Solutions

CNA: Update to 4.0.29 or a higher version.

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

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered 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