WordPress ARMember Plugin <= 4.0.22 is vulnerable to Cross Site Request Forgery (CSRF) leading to PHP Object Injection

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

Summary

CVE	CVE-2023-52200
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-01-08 20:15:44 UTC
Updated	2026-04-28 19:23:02 UTC
Description	Cross-Site Request Forgery (CSRF), Deserialization of Untrusted Data vulnerability in Repute Infosystems ARMember – M

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from nvd@nist.gov

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

EPSS: 0.001950000 probability, percentile 0.412360000 (date 2026-04-28)

Problem Types: CWE-352 | CWE-502 | CWE-352 CWE-352 Cross-Site Request Forgery (CSRF) | CWE-502 CWE-502 Deserialization of Untrusted Data

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	audit@patchstack.com	Secondary	9.6	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H
3.1	CNA	CVSS	9.6	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/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
CNA	Repute Infosystems	ARMember Membership Plugin Content Restriction Member Levels User Profile User Signup	affected n/a 4

References

Reference	Source	Link
patchstack.com/database/vulnerability/armember-membership/wordpress-armember...	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: Rafie Muhammad (Patchstack) (en)

Additional Advisory Data

Solutions

CNA: Update to 4.0.23 or a higher version.

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

Free CVE JSON API cve.report/api

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