



WordPress Aparat for WordPress plugin <= 2.2.0 - Cross Site Scripting (XSS) vulnerability

[MITRE](#)

[NVD](#)

[CVE.ORG](#)

[JSON API](#)

[Print: PDF](#)

Summary

CVE	CVE-2024-29765
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-03-27 14:15:12 UTC
Updated	2026-04-28 19:23:45 UTC
Description	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Alireza Sedghi Aparat 1

Risk And Classification

Primary CVSS: v3.1 6.5 MEDIUM from audit@patchstack.com

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

EPSS: 0.001970000 probability, percentile 0.414920000 (date 2026-04-28)

Problem Types: CWE-79 | CWE-79 CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L
3.1	CNA	CVSS	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

Low

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Alireza Sedghi	Aparat For WordPress	affected n/a 2.2.0 custom	Not specified

References

Reference	Source	Link
patchstack.com/database/vulnerability/wp-aparat/wordpress-aparat-for-wordpre...	af854a3a-2127-422b-91ae-364da2661108	patchstack.c
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Steven Julian (Patchstack Alliance) (en)

Additional Advisory Data

Solutions

CNA: Update to 2.2.1 or a higher version.

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