



WordPress Real3D Flipbook PDF Viewer Lite plugin <= 3.71 - Cross Site Scripting (XSS) vulnerability

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

Summary

CVE	CVE-2024-34561
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-05-08 12:15:09 UTC
Updated	2026-04-28 19:25:26 UTC

Description Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Creative interactive me

Risk And Classification

Primary CVSS: v3.1 5.9 MEDIUM from audit@patchstack.com

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

EPSS: 0.002180000 probability, percentile 0.442920000 (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	5.9	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:L
3.1	CNA	CVSS	5.9	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:L

CVSS v3.1 Breakdown

- Attack Vector: **Network**
- Attack Complexity: **Low**
- Privileges Required: **High**
- User Interaction: **Required**
- Scope: **Changed**
- Confidentiality: **Changed**

Low

Integrity

Low

Availability

Low

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Creative Interactive Media	3D FlipBook PDF Viewer PDF Embedder Real 3D FlipBook WordPress Plugin	affected n/a 3.71 cust

References

Reference	Source	Link
patchstack.com/database/vulnerability/real3d-flipbook-lite/wordpress-real3d-...	af854a3a-2127-422b-91ae-364da2661108	patchstack.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Manab Jyoti Dowarah (Patchstack Alliance) (en)

Additional Advisory Data

Solutions

CNA: Update to 3.72 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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses/mitre).

Free CVE JSON API cve.report/api

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