



# WordPress Product File Upload for WooCommerce plugin <= 2.2.4 - Arbitrary File Deletion vulnerability

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

## Summary

<b>CVE</b>	CVE-2026-25328
<b>State</b>	PUBLISHED
<b>Assigner</b>	Patchstack
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-25 17:16:44 UTC
<b>Updated</b>	2026-04-23 15:37:03 UTC
<b>Description</b>	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in add-ons.org Product File Uplo

## Risk And Classification

**Primary CVSS:** v3.1 6.8 MEDIUM from ADP

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

**EPSS:** 0.000710000 probability, percentile 0.216880000 (date 2026-04-23)

**Problem Types:** CWE-22 | CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	6.8	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N
3.1	audit@patchstack.com	Secondary	6.8	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:N/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	6.8	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N
3.1	CNA	CVSS	6.8	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:N/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

scope

Changed

Confidentiality

High

Integrity

None

Availability

None

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Add-ons.org	Product File Upload For WooCommerce	affected 2.2.4 custom	Not specified

### References

Reference	Source	Link	Tags
patchstack.com/database/Wordpress/Plugin/products-file-upload-for-woocommerc...	audit@patchstack.com	patchstack.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

### Vendor Comments And Credit

Discovery Credit

**CNA:** Denver Jackson | Patchstack Bug Bounty Program (en)

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](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)