



WordPress Folders Plugin <= 2.9.2 is vulnerable to Arbitrary File Upload

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2023-40204 |
| State | PUBLISHED |
| Assigner | Patchstack |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2023-12-20 19:15:09 UTC |
| Updated | 2026-04-28 19:21:08 UTC |
| Description | Unrestricted Upload of File with Dangerous Type vulnerability in Premio Folders – Unlimited Folders to Organize Media Libr |

Risk And Classification

Primary CVSS: v3.1 7.2 HIGH from nvd@nist.gov

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

Problem Types: CWE-434 | CWE-434 CWE-434 Unrestricted Upload of File with Dangerous Type

| Version | Source | Type | Score | Severity | Vector |
|---------|----------------------|-----------|-------|----------|--|
| 3.1 | nvd@nist.gov | Primary | 7.2 | HIGH | CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |
| 3.1 | audit@patchstack.com | Secondary | 9.1 | CRITICAL | CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H |
| 3.1 | CNA | CVSS | 9.1 | CRITICAL | CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H |

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:H/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 | Premio | Folders | All | All | All | All |

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platform |
|--------|--------|---|---------------------------|----------|
| CNA | Premio | Folders Unlimited Folders To Organize Media Library Folder Pages Posts File Manager | affected n/a 2.9.2 custom | No |

References

| Reference | Source | Link |
|---|--------------------------------------|----------------|
| patchstack.com/database/vulnerability/folders/wordpress-folders-plugin-2-9-2... | 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: Rafie Muhammad (Patchstack) (en)

Additional Advisory Data

Solutions

CNA: Update to 2.9.3 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