Folders Pro <= 3.0.2 - Authenticated (Subscriber+) Stored Cross-Site Scripting via User First Name and Last Name

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

Summary

CVE	CVE-2024-3868
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-05-04 03:15:07 UTC
Updated	2026-04-08 19:21:28 UTC
Description	The Folders Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via a user's First Name and Last Name i

Risk And Classification

Primary CVSS: v3.1 5.4 MEDIUM from security@wordfence.com

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

EPSS: 0.002220000 probability, percentile 0.448400000 (date 2026-04-12)

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	security@wordfence.com	Secondary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N
3.1	CNA	DECLARED	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platfo
CNA	Premio	Folders Unlimited Folders To Organize Media Library Folder Pages Posts File Manager	affected 3.0.2 semver	Not sp

References

Reference	Source	Link
premio.io/downloads/folders	af854a3a-2127-422b-91ae-364da2661108	premio.io
www.wordfence.com/threat-intel/vulnerabilities/id/daa48b64-6f89-40be-a31f-31d14...	af854a3a-2127-422b-91ae-364da2661108	www.wor
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

Vendor Comments And Credit

Discovery Credit

CNA: mike harris (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-04-16T00:00:00.000Z	Vendor Notified
CNA	2024-05-03T00:00:00.000Z	Disclosed

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**