



WordPress Frontend File Manager Plugin plugin <= 22.7 - Sensitive Data Exposure vulnerability

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

Summary

CVE	CVE-2024-25903
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-03-17 17:15:06 UTC
Updated	2026-04-28 19:23:29 UTC
Description	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in N-Media Frontend File Manager.This issue affects

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from nvd@nist.gov

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

EPSS: 0.002820000 probability, percentile 0.514910000 (date 2026-04-28)

Problem Types: CWE-200 | NVD-CWE-noinfo | CWE-200 CWE-200 Exposure of Sensitive Information to an Unauthorized Actor

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	audit@patchstack.com	Secondary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
3.1	CNA	CVSS	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Najeebmedia	Frontend File Manager	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	N-Media	Frontend File Manager	affected n/a 22.7 custom	Not specified
ADP	Najeebmedia	Frontend File Manager	affected 22.7 custom	Not specified

References

Reference	Source	Link
patchstack.com/database/vulnerability/nmedia-user-file-uploader/wordpress-fr...	af854a3a-2127-422b-91ae-364da2661108	patchstack.co
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Joshua Chan (Patchstack Alliance) (en)

Additional Advisory Data

Solutions

CNA: Update to 22.8 or a higher version.

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

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