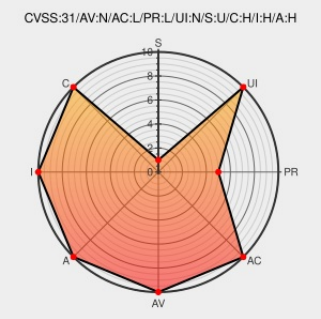
CVE-2022-2356

Published on: Not Yet Published

Last Modified on: 08/11/2022 06:05:00 PM UTC

CVE-2022-2356

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of User Private Files from Mediajedi contain the following vulnerability:

The Frontend File Manager & Sharing WordPress plugin before 1.1.3 does not filter file extensions when letting users upload files on the server, which may lead to malicious code being uploaded.

CVE-2022-2356 has been assigned by contact@wpscan.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Unknown** - **Frontend File Manager & Sharing – User Private Files** version **< 1.1.3**

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
User Private Files < 1.1.3 - Subscriber+ Arbitrary File Upload WordPress Security Vulnerability	web.archive.org text/html Inactive Link Not Archived	MISC wpscan.com/vulnerability/67f3948e-27d4-47a8-8572-616143b9cf43

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mediajedi	User Private Files	All	All	All	All

cpe:2.3:a:mediajedi:user_private_files:*:*:*:*:*:wordpress:*:*:

Discovery Credit

Raad Haddad

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-2356 : The Frontend File Manager & Sharing WordPress plugin before 1.1.3 does not filter file extensions w… twitter.com/i/web/status/1…	2022-08-08 13:57:12
@LinInfoSec	Wordpress - CVE-2022-2356: wpscan.com/vulnerability/…	2022-08-08 17:01:35
@threatmeter	CVE-2022-2356 The Frontend File Manager & Sharing WordPress plugin before 1.1.3 does not filter file extensions whe… twitter.com/i/web/status/1…	2022-08-08 23:21:13
@ColorTokensInc	Emerging Vulnerability Found CVE-2022-2356 - The Frontend File Manager & Sharing WordPress plugin before 1.1.3 does… twitter.com/i/web/status/1…	2022-08-08 23:21:20
@threatmeter	CVE-2022-2356 The Frontend File Manager & Sharing WordPress plugin before 1.1.3 does not filter file extensions whe… twitter.com/i/web/status/1…	2022-08-09 07:09:40
@phpadvisories	CVE-2022-2356 | Frontend File Manager & Sharing Plugin up to 1.1.2 on WordPress File Extension unrestricted upload… twitter.com/i/web/status/1…	2022-08-09 08:22:10
@Har_sia	CVE-2022-2356 har-sia.info/CVE-2022-2356.… #HarsiaInfo	2022-08-10 07:00:08

← Previous ID

Next ID→

© CVE.report 2023 | |
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 registred 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.

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