



CVE-2020-25213

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2020-25213
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-09 16:15:00 UTC
Updated	2023-04-03 20:15:00 UTC
Description	The File Manager (wp-file-manager) plugin before 6.9 for WordPress allows remote attackers to upload and execute arbitra

Risk And Classification

EPSS: 0.944200000 probability, percentile 0.999810000 (date 2026-05-06)

CISA KEV: Listed on 2021-11-03; due 2022-05-03; ransomware use Unknown

Problem Types: CWE-434

CISA Known Exploited Vulnerability

Vendor	WordPress
Product	File Manager Plugin
Name	WordPress File Manager Plugin Remote Code Execution Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2020-25213

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Webdesi9	File Manager	All	All	All	All
Application	Webdesi9	File Manager	All	All	All	All

References

Reference	Source
403 Forbidden	MISC
700,000 WordPress Users Affected by Zero-Day Vulnerability in File Manager Plugin	MISC
Millions of WordPress sites are being probed & attacked with recent plugin bug ZDNet	MISC

File Manager WordPress.org	MISC
WordPress File Manager 6.9 Shell Upload ≈ Packet Storm	MISC
Severe 0-day security vulnerability found by Seravo in WP File Manager Seravo	MISC
WordPress File Manager 6.8 Remote Code Execution ≈ Packet Storm	MISC
WordPress Websites Attacked via File Manager Plugin Vulnerability – HOTforSecurity	MISC
GitHub - w4fz5uck5/wp-file-manager-0day: wp-file-manager 6.7 (Aug 2020) Wordpress Plugin 0day - Remote Code Execution	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD
CISA Known Exploited Vulnerabilities catalog	CISA

No vendor comments have been submitted for this CVE.

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](#)