



CVE-2023-2068

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

Summary

CVE	CVE-2023-2068
State	PUBLIC
Assigner	contact@wpscan.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-27 14:15:00 UTC
Updated	2023-11-07 04:11:00 UTC
Description	The File Manager Advanced Shortcode WordPress plugin through 2.3.2 does not adequately prevent uploading files with di

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Advancedfilemanager	File Manager Advanced Shortcode	All	All	All	All

References

Reference

- [File Manager Advanced Shortcode <= 2.3.2 - Unauthenticated Remote Code Execution through shortcode WordPress Security Vulnerability](#)
- [WordPress File Manager Advanced Shortcode 2.3.2 Remote Code Execution ≈ Packet Storm](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

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](#)