



Media Library Assistant <= 3.09 - Unauthenticated Local/Remote File Inclusion & Remote Code Execution

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

Summary

CVE	CVE-2023-4634
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-06 09:15:08 UTC
Updated	2026-04-08 17:17:03 UTC
Description	The Media Library Assistant plugin for WordPress is vulnerable to Local File Inclusion and Remote Code Execution in versi

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from security@wordfence.com

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

Problem Types: CWE-73 | CWE-73 CWE-73 External Control of File Name or Path

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Davidlingren	Media Library Assistant	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Dglingren	Media Library Assistant	affected 3.09 semver	Not specified

References

Reference	Source
GitHub - Patrowl/CVE-2023-4634: CVE-2023-4634	af854a3a-2127
Media Library Assistant <= 3.09 - Unauthenticated Local/Remote File Inclusion & Remote Code Execution	af854a3a-2127
Blog: CVE-2023-4634 - Tricky Unauthenticated RCE on Wordpress Media Library Assistant Plugin using a good old Imagick	af854a3a-2127
WordPress Media Library Assistant 3.09 LFI / Remote Code Execution ≈ Packet Storm	af854a3a-2127
403 Forbidden	af854a3a-2127
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

CNA: MONTEL (en)

Additional Advisory Data

Source	Time	Event
CNA	2023-09-05T00:00:00.000Z	Disclosed

Legacy QID Mappings

150726 WordPress Media Library Assistant Plugin: Remote Code Execution Vulnerability (CVE-2023-4634)

731059 WordPress Plugin Media Library Assistant Remote Code Execution (RCE) Vulnerability

731067 WordPress Plugin Media Library Assistant Remote Code Execution (RCE) Vulnerability

© [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](#)