



Customized help link for page protection indicator is relative to subpage name, because the link target is missing the "/wiki/" prefix

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

Summary

| | |
|------------------------|------------------------------------------------------------------------------------------------------------------------------|
| CVE | CVE-2026-34094 |
| State | PUBLISHED |
| Assigner | wikimedia-foundation |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-05-11 18:16:32 UTC |
| Updated | 2026-05-12 14:45:49 UTC |
| Description | Vulnerability in Wikimedia Foundation MediaWiki. This vulnerability is associated with program files includes/Page/Article.P |

Risk And Classification

Primary CVSS: v4.0 2 LOW from c4f26cc8-17ff-4c99-b5e2-38fc1793eacc

CVSS:4.0/AV:N/AC:H/AT:P/PR:H/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000390000 probability, percentile 0.115680000 (date 2026-05-12)

Problem Types: CWE-668 | CWE-668 CWE-668 Exposure of Resource to Wrong Sphere

| Version | Source | Type | Score | Severity | Vector |
|---------|--------------------------------------|-----------|-------|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4.0 | c4f26cc8-17ff-4c99-b5e2-38fc1793eacc | Secondary | 2 | LOW | CVSS:4.0/AV:N/AC:H/AT:P/PR:H/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X |
| 4.0 | CNA | CVSS | 2 | LOW | CVSS:4.0/AV:N/AC:H/AT:P/PR:H/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X |

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

Present

Privileges Required

High

User Interaction

Passive

Confidentiality

Low

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:H/AT:P/PR:H/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|--------------------------------------|---------------------------|------------------------------------------|---------------|
| CNA | Wikimedia Foundation | MediaWiki | affected * 1.43.7, 1.44.4, 1.45.2 semver | Not specified |

References

| Reference | Source | Link | Tags |
|-------------------------------------------------------------------------------------------|--------------------------------------|---------------------------------------------------------------------------|---------------------|
| phabricator.wikimedia.org/T416090 | c4f26cc8-17ff-4c99-b5e2-38fc1793eacc | phabricator.wikimedia.org | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

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