



# UserInfoCard: Don't allow access to information about users who are suppressed if you don't have suppressor rights

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

## Summary

<b>CVE</b>	CVE-2025-61647
<b>State</b>	PUBLISHED
<b>Assigner</b>	wikimedia-foundation
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-02-03 00:16:10 UTC
<b>Updated</b>	2026-04-29 01:00:01 UTC
<b>Description</b>	Vulnerability in Wikimedia Foundation CheckUser. This vulnerability is associated with program files src/Api/Rest/Handler/U

## Risk And Classification

**Primary CVSS:** v4.0 0.4 LOW from c4f26cc8-17ff-4c99-b5e2-38fc1793eacc

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

**Problem Types:** CWE-22 | CWE-22 CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Version	Source	Type	Score	Severity	Vector
4.0	c4f26cc8-17ff-4c99-b5e2-38fc1793eacc	Secondary	0.4	LOW	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:A/VC:L/VI:N/VA:N/S
4.0	CNA	CVSS	0.3	LOW	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:A/VC:L/VI:N/VA:N/S

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

Low

User Interaction

Active

Confidentiality

Low

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/E:U/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
CNA	<a href="#">Wikimedia Foundation</a>	<a href="#">CheckUser</a>	affected a3dc1bbcc33acbcca6831d6afaccbb1054c93a57, 0584eb2ad564648aa3ce9c555dd0

### References

Reference	Source	Link	Tags
<a href="https://phabricator.wikimedia.org/T399093">phabricator.wikimedia.org/T399093</a>	<a href="#">c4f26cc8-17ff-4c99-b5e2-38fc1793eacc</a>	<a href="https://phabricator.wikimedia.org">phabricator.wikimedia.org</a>	
CVE Program record	<a href="#">CVE.ORG</a>	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	<a href="#">NVD</a>	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)