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

CVE	CVE-2025-61647
State	PUBLISHED
Assigner	wikimedia-foundation
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-02-03 00:16:10 UTC
Updated	2026-04-29 01:00:01 UTC
Description	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/MSC:X/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	Wikimedia Foundation	CheckUser	affected a3dc1bbcc33acbcca6831d6afaccbb1054c93a57, 0584eb2ad564648aa3ce9c555dd0

References

Reference	Source	Link	Tags
phabricator.wikimedia.org/T399093	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.