Stored XSS through a system message in Special:ApiSandbox

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-67477
State	PUBLISHED
Assigner	wikimedia-foundation
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-02-03 02:16:08 UTC
Updated	2026-04-09 20:32:13 UTC
Description	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Fou

Risk And Classification

Primary CVSS: v4.0 0 NONE from c4f26cc8-17ff-4c99-b5e2-38fc1793eacc

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:N/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

EPSS: 0.000130000 probability, percentile 0.019070000 (date 2026-04-15)

Problem Types: CWE-79 | CWE-79 CWE-79 Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
4.0	c4f26cc8-17ff-4c99-b5e2-38fc1793eacc	Secondary	0	NONE	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:N/VI:N/VA:N/
4.0	CNA	CVSS	0	NONE	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:N/VI:N/VA:N/
3.1	nvd@nist.gov	Primary	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

None

Confidentiality

None

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:N/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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mediawiki	Mediawiki	All	All	All	All
Application	Mediawiki	Mediawiki	1.45.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Wikimedia Foundation	MediaWiki	affected * 1.44.3, 1.45.1 semver	Not specified

References

Reference	Source	Link	Tags
phabricator.wikimedia.org/T406639	c4f26cc8-17ff-4c99-b5e2-38fc1793eacc	phabricator.wikimedia.org	Permissions Required
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.