



CVE-2022-34750

Published on: Not Yet Published

Last Modified on: 07/07/2022 12:39:00 PM UTC

CVE-2022-34750

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Mediawiki](#) from [Mediawiki](#) contain the following vulnerability:

An issue was discovered in MediaWiki through 1.38.1. The lemma length of a Wikibase lexeme is currently capped at a thousand characters. Unfortunately, this length is not validated, allowing much larger lexemes to be created, which introduces various denial-of-service attack vectors within the Wikibase and WikibaseLexeme extensions. This is related to Special:NewLexeme and Special:NewProperty.

CVE-2022-34750 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
No Description Provided	gerrit.wikimedia.org text/html	MISC gerrit.wikimedia.org/r/q/l8171bfef73e525d73efa60b407ce147130ea4742

No Description Provided

gerrit.wikimedia.org

text/html

MISC

gerrit.wikimedia.org/r/q/ld89a9b08e40f075d2d422cafd03668dff3ce7fc9

🔗 T308659 Validate lemma length in Special:NewLexeme(Alpha) and label/description/aliases length in Special:NewProperty

phabricator.wikimedia.org

text/html

MISC

phabricator.wikimedia.org/T308659

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mediawiki	Mediawiki	All	All	All	All
cpe:2.3:a:mediawiki:mediawiki:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
🐦 @CVEreport	CVE-2022-34750 : An issue was discovered in MediaWiki through 1.38.1. The lemma length of a Wikibase lexeme is curr... twitter.com/i/web/status/1...	2022-06-28 13:10:02
🐦 @Inceptus3	New Vulnerability: CVE-2022-34750 #InceptusSecure #UnderOurProtection	2022-06-28 14:17:37
🐦 @0_exploit	CVE-2022-34750 dlvr.it/ST05TP	2022-06-28 14:27:44
🐦 @LinInfoSec	Mediawiki - CVE-2022-34750: gerrit.wikimedia.org/r/q/l8171bfef7...	2022-06-28 16:00:29
🐦 @phpadvisories	CVE-2022-34750 MediaWiki bis 1.38.1 Lemma Length Denial of Service zpr.io/FXYCUTeDpVd3 #phpsec	2022-06-29 15:24:34
🍷 /r/netcve	CVE-2022-34750	2022-06-28 14:38:25

← Previous ID

Next ID →

[site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report