

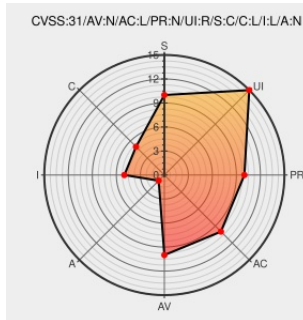


CVE-2020-25828

Published on: 09/27/2020 12:00:00 AM UTC

Last Modified on: 01/01/2022 06:40:00 PM UTC

CVE-2020-25828

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

An issue was discovered in MediaWiki before 1.31.10 and 1.32.x through 1.34.x before 1.34.4. The non-jqueryMsg version of mw.message().parse() doesn't escape HTML. This affects both message contents (which are generally safe) and the parameters (which can be based on user input). (When jqueryMsg is loaded, it

correctly accepts only whitelisted tags in message contents, and escapes all parameters. Situations with an unloaded jqueryMsg are rare in practice, but can for example occur for Special:SpecialPages on a wiki with no extensions installed.)

CVE-2020-25828 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
-------------	------	------

[MediaWiki-I] Security and maintenance release: 1.31.9 / 1.34.3	Mailing List Vendor Advisory lists.wikimedia.org text/html	 CONFIRM lists.wikimedia.org/pipermail/mediawiki-l/2020-September/048480.html
[MediaWiki-I] Maintenance release: 1.31.10 / 1.34.4	Mailing List Vendor Advisory lists.wikimedia.org text/html	 MISC lists.wikimedia.org/pipermail/mediawiki-l/2020-September/048488.html
[SECURITY] Fedora 33 Update: php-oojs-oojs-ui-0.39.3-1.fc33 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2020-a4802c53d9
The MediaWiki-announce Archives	Vendor Advisory lists.wikimedia.org text/html	 MISC lists.wikimedia.org/pipermail/mediawiki-announce

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.

Related QID Numbers

178550 Debian Security Update for mediawiki (DLA 2379-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Mediawiki	Mediawiki	All	All	All	All
Application	Mediawiki	Mediawiki	1.31.10	All	All	All
Application	Mediawiki	Mediawiki	All	All	All	All
Application	Mediawiki	Mediawiki	1.31.10	All	All	All
cpe:2.3:o:fedoraproject:fedora:33:*****:						
cpe:2.3:a:mediawiki:mediawiki:*****:						
cpe:2.3:a:mediawiki:mediawiki:1.31.10:*****:						
cpe:2.3:a:mediawiki:mediawiki:*****:						
cpe:2.3:a:mediawiki:mediawiki:1.31.10:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023  |

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)