

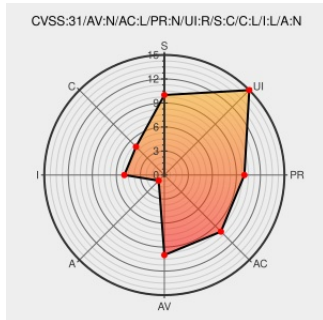


CVE-2020-25812

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

Last Modified on: 01/01/2022 06:39:00 PM UTC

CVE-2020-25812

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

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

An issue was discovered in MediaWiki 1.34.x before 1.34.4. On Special:Contributions, the NS filter uses unescaped messages as keys in the option key for an HTMLForm specifier. This is vulnerable to a mild XSS if one of those messages is changed to include raw HTML.

CVE-2020-25812 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
includes/specials/SpecialContributions.php - mediawiki/core - Gitiles	Vendor Advisory gerrit.wikimedia.org text/html	MISC gerrit.wikimedia.org/g/mediawiki/core/+/ad4a3ba45fb955aa8c0eb3c8380/
[MediaWiki-l] Security and maintenance	Mailing List	CONFIRM lists.wikimedia.org/pipermail/mediawiki-l/2020-September/

release: 1.31.9 / 1.34.3

Vendor Advisory

lists.wikimedia.org

text/html

[MediaWiki-l] 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/0484

[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

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
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Mediawiki	Mediawiki	All	All	All	All
Application	Mediawiki	Mediawiki	All	All	All	All

cpe:2.3:o:fedoraproject:fedora:33:*****:

cpe:2.3:a:mediawiki:mediawiki:*****:

cpe:2.3:a:mediawiki:mediawiki:*****:

No vendor comments have been submitted for this CVE

Social Mentions

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

← Previous ID

Next ID →