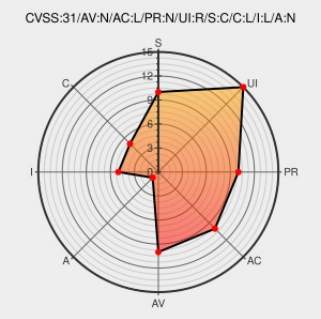
CVE-2020-35479

Published on: 12/18/2020 12:00:00 AM UTC

Last Modified on: 10/05/2022 04:09:00 PM UTC

CVE-2020-35479

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Debian Linux from Debian contain the following vulnerability:

MediaWiki before 1.35.1 allows XSS via BlockLogFormatter.php. Language::translateBlockExpiry itself does not escape in all code paths. For example, the return of Language::userTimeAndDate is is always unsafe for HTML in a month value. This affects MediaWiki 1.12.0 and later.

CVE-2020-35479 has been assigned by 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
Debian -- Security Information -- DSA-4816-1 mediawiki	Third Party Advisory www.debian.org Depreciated Link	DEBIAN DSA-4816

	text/html	
[MediaWiki-announce] Security and maintenance release: 1.31.11 / 1.35.1	Mailing List Release Notes Vendor Advisory lists.wikimedia.org text/html	MISC lists.wikimedia.org/pipermail/mediawiki-announce/2020-December/000268.html
[SECURITY] Fedora 33 Update: mediawiki-1.35.1-1.fc33 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2020-0be2d40e13
⚓ T268938 BlockLogFormatter can output raw html (CVE-2020-35478, CVE-2020-35479)	Exploit Vendor Advisory phabricator.wikimedia.org text/html	MISC phabricator.wikimedia.org/T268938
[SECURITY] [DLA 2504-1] mediawiki security update	Mailing List Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20201223 [SECURITY] [DLA 2504-1] mediawiki security update

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	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
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:debian:debian_linux:10.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

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)
@RemotelyAlerts	Severity: ?? | MediaWiki before 1.35.1 allows XSS via B... | CVE-2020-35479 | Link for more: alerts.remotelyrmm.com/CVE-2020-35479	2022-10-05 17:31:39

← 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 registred 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