



CVE-2012-4378

Published on: 10/26/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:15 PM UTC

CVE-2012-4378

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

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

Multiple cross-site scripting (XSS) vulnerabilities in MediaWiki before 1.18.5 and 1.19.x before 1.19.2, when unspecified JavaScript gadgets are used, allow remote attackers to inject arbitrary web script or HTML via the userlang parameter to w/index.php.

CVE-2012-4378 has been assigned by secalert@redhat.com 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
⚓ T39587 character filter for uselang	Issue Tracking Patch Vendor Advisory phabricator.wikimedia.org text/html	CONFIRM phabricator.wikimedia.org/T39587

oss-security - CVE Request -- MediaWiki 1.19.2 and 1.18.5 multiple security flaws	Mailing List Patch Third Party Advisory www.openwall.com text/html	 MLIST [oss-security] 20120831 CVE Request -- MediaWiki 1.19.2 and 1.18.5 multiple security flaws
853417 – (CVE-2012-4378) CVE-2012-4378 mediawiki: Multiple DOM-based XSS flaws due improper filtering of uselang parameter	Issue Tracking Patch Third Party Advisory bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=853417
#686330 - mediawiki: Multiple security issues CVE-2012-4377,CVE-2012-4378,CVE-2012-4379,CVE-2012-4380,CVE-2012-4381,CVE-2012-4382 - Debian Bug report logs	Issue Tracking Third Party Advisory bugs.debian.org text/html	 MISC bugs.debian.org/cgi-bin/bugreport.cgi?bug=686330
oss-security - Re: CVE Request -- MediaWiki 1.19.2 and 1.18.5 multiple security flaws	Mailing List Patch Third Party Advisory www.openwall.com text/html	 MLIST [oss-security] 20120831 Re: CVE Request -- MediaWiki 1.19.2 and 1.18.5 multiple security flaws
[MediaWiki-announce] MediaWiki security release: 1.19.2 and 1.18.5	Patch Vendor Advisory lists.wikimedia.org text/html	 MLIST [MediaWiki-announce] 20120831 MediaWiki security release: 1.19.2 and 1.18.5

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	1.19.0	All	All	All
Application	Mediawiki	Mediawiki	1.19.1	All	All	All
Application	Mediawiki	Mediawiki	1.19.0	All	All	All
Application	Mediawiki	Mediawiki	1.19.1	All	All	All
Application	Mediawiki	Mediawiki	All	All	All	All
cpe:2.3:a:mediawiki:mediawiki:1.19.0:*:*:*:*:*:						
cpe:2.3:a:mediawiki:mediawiki:1.19.1:*:*:*:*:*:						
cpe:2.3:a:mediawiki:mediawiki:1.19.0:*:*:*:*:*:						
cpe:2.3:a:mediawiki:mediawiki:1.19.1:*:*:*:*:*:						
cpe:2.3:a:mediawiki:mediawiki:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

No further comments have been submitted for this CVE

[← 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](#)