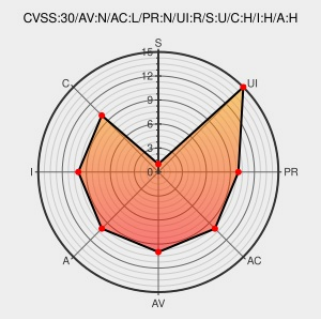
CVE-2015-8624

Published on: 03/23/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:14 PM UTC

CVE-2015-8624

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



Certain versions of Mediawiki from Mediawiki contain the following vulnerability:

The User::matchEditToken function in includes/User.php in MediaWiki before 1.23.12, 1.24.x before 1.24.5, 1.25.x before 1.25.4, and 1.26.x before 1.26.1 does not perform token comparison in constant time before determining if a debugging message should be logged, which allows remote attackers to guess the edit token and bypass CSRF protection via a timing attack, a different vulnerability than CVE-2015-8623.

CVE-2015-8624 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
oss-security - CVE requests for MediaWiki 1.26.1, 1.25.4, 1.24.5 and 1.23.12	Mailing List, Patch	MLIST [oss-security] 20151221 CVE requests for MediaWiki 1.26.1, 1.25.4, 1.24.5 and 1.23.12

	Third Party Advisory www.openwall.com text/html	
⚓ T119309 User::matchEditToken should use constant-time string comparison	Patch Third Party Advisory phabricator.wikimedia.org text/html	CONFIRM phabricator.wikimedia.org/T119309
[MediaWiki-announce] Security Release: 1.26.1, 1.25.4, 1.24.5 and 1.23.12	Patch Release Notes Vendor Advisory lists.wikimedia.org text/html	MLIST [MediaWiki-announce] 20151221 [MediaWiki-announce] Security Release: 1.26.1, 1.25.4, 1.24.5 and 1.23.12
oss-security - Re: CVE requests for MediaWiki 1.26.1, 1.25.4, 1.24.5 and 1.23.12	Mailing List Patch Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20151223 Re: CVE requests for MediaWiki 1.26.1, 1.25.4, 1.24.5 and 1.23.12

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	1.24.0	All	All	All
Application	Mediawiki	Mediawiki	1.24.1	All	All	All
Application	Mediawiki	Mediawiki	1.24.2	All	All	All
Application	Mediawiki	Mediawiki	1.24.3	All	All	All
Application	Mediawiki	Mediawiki	1.24.4	All	All	All
Application	Mediawiki	Mediawiki	1.25.0	All	All	All
Application	Mediawiki	Mediawiki	1.25.1	All	All	All
Application	Mediawiki	Mediawiki	1.25.2	All	All	All
Application	Mediawiki	Mediawiki	1.25.3	All	All	All
Application	Mediawiki	Mediawiki	1.26.0	All	All	All
Application	Mediawiki	Mediawiki	1.24.0	All	All	All
Application	Mediawiki	Mediawiki	1.24.1	All	All	All
Application	Mediawiki	Mediawiki	1.24.2	All	All	All
Application	Mediawiki	Mediawiki	1.24.3	All	All	All
Application	Mediawiki	Mediawiki	1.24.4	All	All	All
Application	Mediawiki	Mediawiki	1.25.0	All	All	All
Application	Mediawiki	Mediawiki	1.25.1	All	All	All

Application	Mediawiki	Mediawiki	1.25.2	All	All	All
Application	Mediawiki	Mediawiki	1.25.3	All	All	All
Application	Mediawiki	Mediawiki	1.26.0	All	All	All
Application	Mediawiki	Mediawiki	All	All	All	All

cpe:2.3:a:mediawiki:mediawiki:1.24.0:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.24.1:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.24.2:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.24.3:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.24.4:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.25.0:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.25.1:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.25.2:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.25.3:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.26.0:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.24.0:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.24.1:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.24.2:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.24.3:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.24.4:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.25.0:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.25.1:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.25.2:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.25.3:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.26.0:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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