



CVE-2015-8009

Published on: 07/25/2017 12:00:00 AM UTC

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

CVE-2015-8009

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

The MWOAuthDataStore::lookup_token function in Extension:OAuth for MediaWiki 1.25.x before 1.25.3, 1.24.x before 1.24.4, and before 1.23.11 does not properly validate the signature when checking the authorization signature, which allows remote registered Consumers to use another Consumer's credentials by leveraging knowledge of the

credentials.

CVE-2015-8009 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
oss-security - Re: CVE Request: MediaWiki 1.25.3, 1.24.4 and 1.23.11	Mailing List VDB Entry	MLIST [oss-security] 20151029 Re: CVE Request: MediaWiki

1.25.3, 1.24.4 and 1.23.11

MediaWiki Multiple Bugs Let Remote Users Obtain Potentially Sensitive Information and Conduct Cross-Site Scripting Attacks and Let Remote Authenticated Users Bypass Security and Deny Service - SecurityTracker

www.securitytracker.com

text/html

 SECTRAK 1034028

🔗 T103023 API requests don't get validated if signed by the correct OAuth consumer

```
Exploit
Third Party Advisory
phabricator.wikimedia.org
text/html
```

 CONFIRM
phabricator.wikimedia.org/T103023

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
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	1.25.0	All	All	All
Application	Mediawiki	Mediawiki	1.25.1	All	All	All
Application	Mediawiki	Mediawiki	1.25.2	All	All	All
Application	Mediawiki	Mediawiki	1.24.0	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	1.25.0	All	All	All
Application	Mediawiki	Mediawiki	1.25.1	All	All	All
Application	Mediawiki	Mediawiki	1.25.2	All	All	All
Application	Mediawiki	Mediawiki	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:1.25.0:*:*:*:*:*:						

cpe:2.3:a:mediawiki:mediawiki:1.25.1:*.~::~
cpe:2.3:a:mediawiki:mediawiki:1.25.2:*.~::~
cpe:2.3:a:mediawiki:mediawiki:1.24.0:*.~::~
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:1.25.0:*.~::~
cpe:2.3:a:mediawiki:mediawiki:1.25.1:*.~::~
cpe:2.3:a:mediawiki:mediawiki:1.25.2:*.~::~
cpe:2.3:a:mediawiki:mediawiki:*.~::~

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)