



CVE-2006-2895

Published on: 06/07/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:08 PM UTC

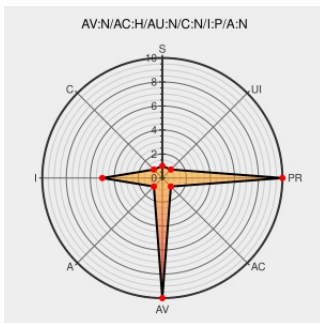
CVE-2006-2895

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

Cross-site scripting (XSS) vulnerability in MediaWiki 1.6.0 up to versions before 1.6.7 allows remote attackers to inject arbitrary HTML and web script via the edit form.

CVE-2006-2895 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **2.6 - LOW**

**Access
Vector**

NETWORK

**Access
Complexity**

HIGH

Authentication

NONE

**Confidentiality
Impact**

NONE

**Integrity
Impact**

PARTIAL

**Availability
Impact**

NONE

CVE References

Description

Tags

Link

MediaWiki Edit Form Script
Insertion Vulnerability - Advisories
- Secunia

[Patch](#)
[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)

[X](#) [SECUNIA 20458](#)

Query: Hosted in Phabricator

[Patch](#)
[svn.wikimedia.org](#)
[text/html](#)

[G](#) [CONFIRM](#)
[svn.wikimedia.org/viewvc/mediawiki/tags/REL1_6_7/phase3/RELEASE-NOTES](#)

[MediaWiki-announce] MediaWiki
1.6.7 released

[Patch](#)
[mail.wikipedia.org](#)
[text/html](#)

[M](#) [MLIST \[MediaWiki-announce\] 20060606 MediaWiki 1.6.7 released](#)

Webmail : Solution de messagerie
professionnelle - OVHcloud- OVH

[www.vupen.com](#)
[text/html](#)

[G](#) [VUPEN ADV-2006-2159](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)

[X](#) [XF mediawiki-edit-form-xss\(27029\)](#)

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	1.6.0	All	All	All
Application	Mediawiki	Mediawiki	1.6.1	All	All	All
Application	Mediawiki	Mediawiki	1.6.2	All	All	All
Application	Mediawiki	Mediawiki	1.6.3	All	All	All
Application	Mediawiki	Mediawiki	1.6.4	All	All	All
Application	Mediawiki	Mediawiki	1.6.5	All	All	All
Application	Mediawiki	Mediawiki	1.6.5_r14348	All	All	All
Application	Mediawiki	Mediawiki	1.6.6	All	All	All
Application	Mediawiki	Mediawiki	1.6.0	All	All	All
Application	Mediawiki	Mediawiki	1.6.1	All	All	All
Application	Mediawiki	Mediawiki	1.6.2	All	All	All
Application	Mediawiki	Mediawiki	1.6.3	All	All	All
Application	Mediawiki	Mediawiki	1.6.4	All	All	All
Application	Mediawiki	Mediawiki	1.6.5	All	All	All
Application	Mediawiki	Mediawiki	1.6.5_r14348	All	All	All
Application	Mediawiki	Mediawiki	1.6.6	All	All	All

```
cpe:2.3:a:mediawiki:mediawiki:1.6.0:*:*:*:*:*:
```

```
cpe:2.3:a:mediawiki:mediawiki:1.6.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:mediawiki:mediawiki:1.6.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:mediawiki:mediawiki:1.6.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:mediawiki:mediawiki:1.6.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:mediawiki:mediawiki:1.6.5:*:*:*:*:*:
```

cpe:2.3:a:mediawiki:mediawiki:1.6.5_r14348.*:*:*:*:*:*:

```
cpe:2.3:a:mediawiki:mediawiki:1.6.6:*:*:*:*:*:*:
```

```
cpe:2.3-a:mediawiki:mediawiki-1.6.0:*.*.*.*.*.*.*.*
```

cpe:2.3:a:mediawiki:mediawiki:1.6.0:*****:
cpe:2.3:a:mediawiki:mediawiki:1.6.1:*****:
cpe:2.3:a:mediawiki:mediawiki:1.6.2:*****:
cpe:2.3:a:mediawiki:mediawiki:1.6.3:*****:
cpe:2.3:a:mediawiki:mediawiki:1.6.4:*****:
cpe:2.3:a:mediawiki:mediawiki:1.6.5:*****:
cpe:2.3:a:mediawiki:mediawiki:1.6.5_r14348:*****:
cpe:2.3:a:mediawiki:mediawiki:1.6.6:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →