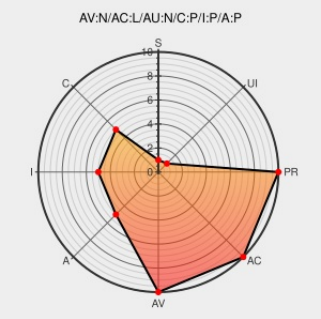
CVE-2004-1405

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:10 PM UTC

CVE-2004-1405

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



Certain versions of Mediawiki from Mediawiki contain the following vulnerability:

MediaWiki 1.3.8 and earlier, when used with Apache mod_mime, does not properly handle files with two file extensions, such as .php.rar, which allows remote attackers to upload and execute arbitrary code.

CVE-2004-1405 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
'STG Security Advisory: [SSA-20041215-19] Vulnerability of' - MARC	marc.info, text/html	BUGTRAQ 20041216 STG Security Advisory: [SSA-20041215-19] Vulnerability of uploading files with multiple extensions in MediaWiki
MediaWiki Remote Arbitrary Script Upload Vulnerability	Exploit, Patch, cve.report (archive), text/html	BID 11985
MediaWiki development	Patch, wikipedia.sourceforge.net, text/html	MISC wikipedia.sourceforge.net/
Secunia - Advisories - MoniWiki Multiple File Extensions Script Upload Vulnerability	web.archive.org, text/html	SECUNIA 13478

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	1.3	All	All	All
Application	Mediawiki	Mediawiki	1.3.0	All	All	All
Application	Mediawiki	Mediawiki	1.3.1	All	All	All
Application	Mediawiki	Mediawiki	1.3.10	All	All	All
Application	Mediawiki	Mediawiki	1.3.11	All	All	All
Application	Mediawiki	Mediawiki	1.3.2	All	All	All
Application	Mediawiki	Mediawiki	1.3.3	All	All	All
Application	Mediawiki	Mediawiki	1.3.4	All	All	All
Application	Mediawiki	Mediawiki	1.3.5	All	All	All
Application	Mediawiki	Mediawiki	1.3.6	All	All	All
Application	Mediawiki	Mediawiki	1.3.7	All	All	All
Application	Mediawiki	Mediawiki	1.3.8	All	All	All
Application	Mediawiki	Mediawiki	1.3	All	All	All
Application	Mediawiki	Mediawiki	1.3.0	All	All	All
Application	Mediawiki	Mediawiki	1.3.1	All	All	All
Application	Mediawiki	Mediawiki	1.3.10	All	All	All
Application	Mediawiki	Mediawiki	1.3.11	All	All	All
Application	Mediawiki	Mediawiki	1.3.2	All	All	All
Application	Mediawiki	Mediawiki	1.3.3	All	All	All
Application	Mediawiki	Mediawiki	1.3.4	All	All	All
Application	Mediawiki	Mediawiki	1.3.5	All	All	All
Application	Mediawiki	Mediawiki	1.3.6	All	All	All
Application	Mediawiki	Mediawiki	1.3.7	All	All	All
Application	Mediawiki	Mediawiki	1.3.8	All	All	All

cpe:2.3:a:mediawiki:mediawiki:1.3:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.3.10:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.3.11:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.3.3:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.3.4:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.3.5:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.3.6:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.3.7:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.3.8:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.3:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.3.10:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.3.11:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.3.3:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.3.4:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.3.5:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.3.6:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.3.7:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.3.8:*:*:*:*:*:*:*:

No vendor 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 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