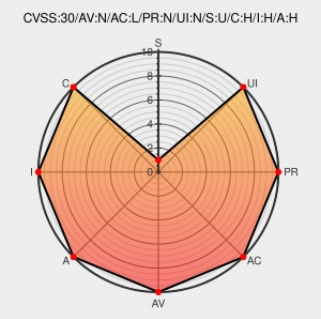
CVE-2017-8809

Published on: 11/15/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:42 PM UTC

CVE-2017-8809

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



Certain versions of Debian Linux from Debian contain the following vulnerability:

api.php in MediaWiki before 1.27.4, 1.28.x before 1.28.3, and 1.29.x before 1.29.2 has a Reflected File Download vulnerability.

CVE-2017-8809 has been assigned by security@debian.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: 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
[MediaWiki-announce] Security release: 1.29.2 / 1.28.3 / 1.27.4	Mailing List, Patch, Vendor Advisory, lists.wikimedia.org, text/html	CONFIRM lists.wikimedia.org/pipermail/mediawiki-announce/2017-November/000216.html

Debian -- Security Information -- DSA-4036-1 mediawiki	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-4036
MediaWiki Multiple Flaws Let Remote Users Modify Data, Obtain Potentially Sensitive Information, and Conduct Cross-Site Scripting Attacks and Let Local Users Obtain Passwords - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1039812

There are currently no QIDs associated with this CVE

Exploit/POC from Github

CVE-2017-8809 Docker - RFD(Reflected File Download) for MediaWiki

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Mediawiki	Mediawiki	1.28.0	All	All	All
Application	Mediawiki	Mediawiki	1.28.1	All	All	All
Application	Mediawiki	Mediawiki	1.28.2	All	All	All
Application	Mediawiki	Mediawiki	1.29.0	All	All	All
Application	Mediawiki	Mediawiki	1.29.1	All	All	All
Application	Mediawiki	Mediawiki	1.28.0	All	All	All
Application	Mediawiki	Mediawiki	1.28.1	All	All	All
Application	Mediawiki	Mediawiki	1.28.2	All	All	All
Application	Mediawiki	Mediawiki	1.29.0	All	All	All
Application	Mediawiki	Mediawiki	1.29.1	All	All	All
Application	Mediawiki	Mediawiki	All	All	All	All

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.28.0:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.28.1:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.28.2:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.29.0:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.29.1:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.28.0:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.28.1:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.28.2:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.29.0:*:*:*:*:*:*:*:

cpe:2.3:a:mediawiki:mediawiki:1.29.1:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→