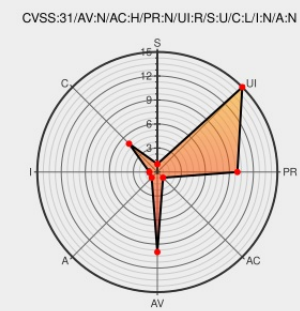
CVE-2020-15005

Published on: 06/24/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-15005

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



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

In MediaWiki before 1.31.8, 1.32.x and 1.33.x before 1.33.4, and 1.34.x before 1.34.2, private wikis behind a caching server using the img_auth.php image authorization security feature may have had their files cached publicly, so any unauthorized user could view them. This occurs because Cache-Control and Vary headers were mishandled.

CVE-2020-15005 has been assigned by cve@mitre.org to track the vulnerability - currently rated as LOW severity.

CVSS3 Score: 3.1 - LOW

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

CVSS2 Score: 2.6 - LOW

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

CVE References

Description	Tags	Link
[Wikitech-l] Security and maintenance release: 1.31.8 / 1.33.4 / 1.34.2	Mailing List Release Notes Vendor Advisory	CONFIRM lists.wikimedia.org/pipermail/wikitech-l/2020-June/093535.html

	lists.wikimedia.org text/html	
Debian -- Security Information -- DSA-4767-1 mediawiki	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-4767
RELEASE-NOTES-1.31 - mediawiki/core - Gitiles	Release Notes Vendor Advisory gerrit.wikimedia.org text/html	CONFIRM gerrit.wikimedia.org/r/plugins/gitiles/mediawiki/core/+/REL1_31/RELEASE-NOTES-1.31
⚓ T248947 img_auth.php may leak private extension images into the public cache (CVE-2020-15005)	Patch Vendor Advisory phabricator.wikimedia.org text/html	MISC phabricator.wikimedia.org/T248947
[SECURITY] Fedora 32 Update: mediawiki-1.33.4-1.fc32 - package-announce - Fedora Mailing-Lists	Third Party Advisory lists.fedoraproject.org text/html	FEDORA FEDORA-2020-9c97633708
[SECURITY] [DLA 2504-1] mediawiki security update	Mailing List Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20201223 [SECURITY] [DLA 2504-1] mediawiki security update
RELEASE-NOTES-1.33 - mediawiki/core - Gitiles	Release Notes Vendor Advisory gerrit.wikimedia.org text/html	CONFIRM gerrit.wikimedia.org/r/plugins/gitiles/mediawiki/core/+/REL1_33/RELEASE-NOTES-1.33
RELEASE-NOTES-1.34 - mediawiki/core - Gitiles	Release Notes Vendor Advisory gerrit.wikimedia.org text/html	CONFIRM gerrit.wikimedia.org/r/plugins/gitiles/mediawiki/core/+/REL1_34/RELEASE-NOTES-1.34

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All

System

Application	Mediawiki	Mediawiki	All	All	All	All
Application	Mediawiki	Mediawiki	All	All	All	All

cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:*:*:

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

cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:*:*:

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

cpe:2.3:o:fedoraproject:fedora:32:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:32:*:*:*:*:*:*:*:

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→