



# CVE-2020-15005

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

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

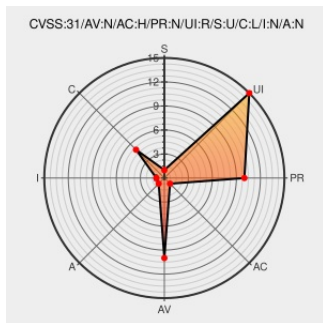
## CVE-2020-15005

[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 [M](#) [cve@mitre.org](mailto: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    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>HIGH</b>            | <b>NONE</b>         | <b>REQUIRED</b>     |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |

CVSS2 Score: **2.6 - LOW**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>HIGH</b>       | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>PARTIAL</b>         | <b>NONE</b>       | <b>NONE</b>         |

## CVE References

| Description                                                             | Tags                                                                                             | Link                                                                                                                                                               |
|-------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [Wikitech-l] Security and maintenance release: 1.31.8 / 1.33.4 / 1.34.2 | <a href="#">Mailing List</a><br><a href="#">Release Notes</a><br><a href="#">Vendor Advisory</a> | <a href="mailto:CONFIRM@lists.wikimedia.org/pipermail/wikitech-l/2020-June/093535.html">CONFIRM lists.wikimedia.org/pipermail/wikitech-l/2020-June/093535.html</a> |

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

By selecting these links, you may be leaving CVEreport webospace. 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](mailto: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 |
| Operating System                         | <a href="#">Debian</a>        | <a href="#">Debian Linux</a> | 10.0    | All    | All     | All      |
| Operating System                         | <a href="#">Debian</a>        | <a href="#">Debian Linux</a> | 9.0     | All    | All     | All      |
| Operating System                         | <a href="#">Debian</a>        | <a href="#">Debian Linux</a> | 10.0    | All    | All     | All      |
| Operating System                         | <a href="#">Debian</a>        | <a href="#">Debian Linux</a> | 9.0     | All    | All     | All      |
| Operating System                         | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>       | 32      | All    | All     | All      |
| Operating System                         | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>       | 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 |           |           |                           |     |     |     |
| <a href="#">← Previous ID</a>                       |           |           | <a href="#">Next ID →</a> |     |     |     |