

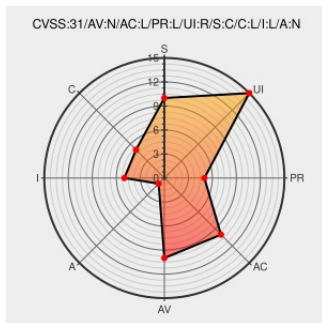


CVE-2019-16216

Published on: 09/18/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:49 PM UTC

CVE-2019-16216

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

Zulip server before 2.0.5 incompletely validated the MIME types of uploaded files. A user who is logged into the server could upload files of certain types to mount a stored cross-site scripting attack on other logged-in users. On a Zulip server using the default local uploads backend, the attack is only effective against browsers lacking support

for Content-Security-Policy such as Internet Explorer 11. On a Zulip server using the S3 uploads backend, the attack is confined to the origin of the configured S3 uploads hostname and cannot reach the Zulip server itself.

CVE-2019-16216 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.4 - MEDIUM**

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

CVSS2 Score: **3.5 - LOW**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
-------------	------	------

CVE-2019-16216: Fix MIME type validation. · zulip/zulip@1195841 · GitHub

[Patch](#)
[Third Party Advisory](#)
[github.com](#)
[text/html](#)

 **CONFIRM**
github.com/zulip/zulip/commit/1195841dfb9aa26b3b0dabc6f05d72e4af25be3e

Zulip Server 2.0.5 security release

[Vendor Advisory](#)
[blog.zulip.org](#)
[text/html](#)

 **CONFIRM** blog.zulip.org/2019/09/11/zulip-server-2-0-5-security-release/

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	Zulip	Zulip Server	All	All	All	All
Application	Zulip	Zulip Server	All	All	All	All
cpe:2.3:a:zulip:zulip_server:*****:						
cpe:2.3:a:zulip:zulip_server:*****:						

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 registered 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](#)