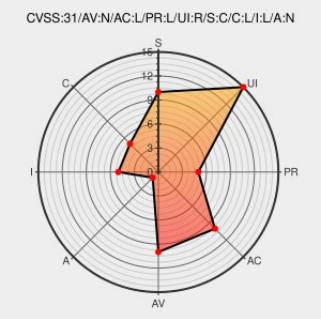
CVE-2019-16216

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 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/

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→