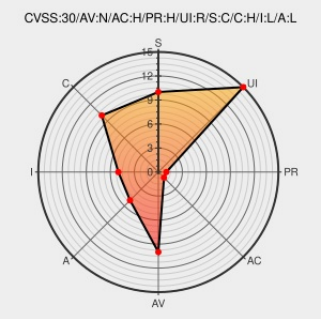
CVE-2021-3866

Published on: 01/20/2022 12:00:00 AM UTC

Last Modified on: 02/03/2022 02:20:00 PM UTC

CVE-2021-3866 - advisory for 5f48dac5-e112-4b23-bbbf-cc00ba83bcf2

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



Certain versions of Zulip from Zulip contain the following vulnerability:

Cross-site Scripting (XSS) - Stored in GitHub repository zulip/zulip more than and including 44f935695d452cc3fb16845a0c6af710438b153d and prior to 3eb2791c3e9695f7d37ffe84e0c2184fae665cb6.

CVE-2021-3866 has been assigned by security@huntr.dev to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **zulip** - **zulip/zulip** version **>= 44f935695d452cc3fb16845a0c6af710438b153d**

Affected Vendor/Software: **zulip** - **zulip/zulip** version **< 3eb2791c3e9695f7d37ffe84e0c2184fae665cb6**

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

Cross-site Scripting (XSS) - Stored vulnerability found in zulip	huntr.dev text/html	CONFIRM huntr.dev/bounties/5f48dac5-e112-4b23-bbbf-ccd0ba83bcf2
CVE-2021-3853: Fix HTML escaping in recipient_row. · zulip/zulip@3eb2791 · GitHub	github.com text/html	MISC github.com/zulip/zulip/commit/3eb2791c3e9695f7d37ffe84e0c2184fae665cb6
CVE-2021-3866: XSS in stream names	blog.zulip.com text/html	MISC blog.zulip.com/2022/01/19/cve-2021-3866/

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	All	All	All	All

cpe:2.3:a:zulip:zulip:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-3866 : Cross-site Scripting #XSS - Stored in GitHub repository zulip/zulip prior to main.... cve.report/CVE-2021-3866	2022-01-20 10:35:22
@OpenSourceHacks	(CVE-2021-3866): Cross-site Scripting (XSS) - Stored in zulip/zulip. huntr.dev/bounties/5f48d… Disclosed by… twitter.com/i/web/status/1…	2022-01-20 11:30:19
/r/netcve	CVE-2021-3866	2022-01-20 11:38:26

← Previous ID

Next ID→