



CVE-2022-35962

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2022-35962 |
| State | PUBLIC |
| Assigner | security-advisories@github.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2022-08-29 15:15:00 UTC |
| Updated | 2022-09-07 18:48:00 UTC |
| Description | Zulip is an open source team chat and Zulip Mobile is an app for iOS and Andriod users. In Zulip Mobile through version 27 |

Risk And Classification

Problem Types: CWE-697

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|-----------------------|-----------------------|---------|--------|---------|----------|
| Application | Zulip | Zulip | All | All | All | All |
| Application | Zulip | Zulip | All | All | All | All |

References

| Reference | Source | Link | Tags |
|--|---------|---|------|
| Zulip Server 5.6 security release | MISC | blog.zulip.com | |
| Crafted link in Zulip message can cause disclosure of credentials · Advisory · zulip/zulip-mobile · GitHub | CONFIRM | github.com | |
| Release v27.190 · zulip/zulip-mobile · GitHub | MISC | github.com | |
| CVE Program record | CVE.ORG | www.cve.org | cano |
| NVD vulnerability detail | NVD | nvd.nist.gov | cano |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#)