



CVE-2020-10935

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#) 

Summary

CVE	CVE-2020-10935
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-20 20:15:00 UTC
Updated	2020-04-28 18:57:00 UTC
Description	Zulip Server before 2.1.3 allows XSS via a Markdown link, with resultant account takeover.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zulip	Zulip Server	All	All	All	All
Application	Zulip	Zulip Server	All	All	All	All

References

Reference	Source	Link	Tags
Zulip server 2.1.3 security release	CONFIRM	blog.zulip.org	Vendor Advisory
CoreLabs Advisories - Zulip Account Takeover Via Stored XSS Core Security	MISC	www.coresecurity.com	Exploit, Third Party Ac
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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](#)