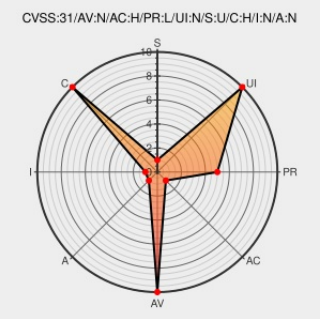
CVE-2022-45195

Published on: Not Yet Published

Last Modified on: 11/17/2022 05:06:00 PM UTC

CVE-2022-45195

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



Certain versions of Simplexmq from Simplex contain the following vulnerability:

SimpleXMQ before 3.4.0, as used in SimpleX Chat before 4.2, does not apply a key derivation function to intended data, which can interfere with forward secrecy and can have other impacts if there is a compromise of a single private key. This occurs in the X3DH key exchange for the double ratchet protocol.

CVE-2022-45195 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.3 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	NONE

CVE References

Description	Tags	Link
publications/SimpleXChat.pdf at master · trailofbits/publications · GitHub	github.com text/html	MISC github.com/trailofbits/publications/blob/master/reviews/SimpleXChat.pdf
Comparing v3.3.0...v3.4.0 · simplex-chat/simplexmq · GitHub	github.com text/html	MISC github.com/simplex-chat/simplexmq/compare/v3.3.0...v3.4.0
use KDF in X3DH by epoberezkin · Pull Request #548 · simplex-chat/simplexmq · GitHub	github.com text/html	MISC github.com/simplex-chat/simplexmq/pull/548
SimpleX blog: Security assessment by Trail of Bits, the new website and v4.2 released	simplex.chat text/html	MISC simplex.chat/blog/20221108-simplex-chat-v4.2-security-audit-new-website.html

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	Simplex	Simplexmq	All	All	All	All
Application	Simplex	Simplex Chat	All	All	All	All

cpe:2.3:a:simplex:simplexmq:*:*:*:*:*:*:*:*:

cpe:2.3:a:simplex:simplex_chat:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-45195 : SimpleXMQ before 3.4.0, as used in SimpleX Chat before 4.2, does not apply a key derivation functi… twitter.com/i/web/status/1…	2022-11-12 19:04:16
/r/netcve	CVE-2022-45195	2022-11-12 20:38:42

← Previous ID

Next ID→