exists for "<" or ">" but escaping for double quotes does not exist. Through this vulnerability, an attacker is capable to execute malicious scripts. Users are advised to update as soon as possible." />

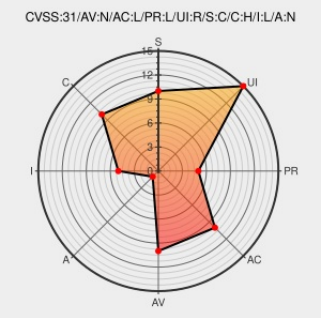
CVE-2022-21649

Published on: 01/04/2022 12:00:00 AM UTC

Last Modified on: 01/08/2022 02:46:00 AM UTC

CVE-2022-21649 - advisory for GHSA-xmpj-xwm3-vww7

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



Certain versions of Convos from Convos contain the following vulnerability:

Convos is an open source multi-user chat that runs in a web browser. Characters starting with "https://" in the chat window create an <a> tag. Stored XSS vulnerability using onfocus and autofocus occurs because escaping exists for "<" or ">" but escaping for double quotes does not exist. Through this vulnerability, an attacker is capable to execute malicious scripts. Users are advised to update as soon as possible.

CVE-2022-21649 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **convos-chat** - **convos** version **>= 6.49, < 6.52**

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
Fix XSS vulnerability in links and changed I18N.md() to be understand… · convos-chat/convos@86b2193 · GitHub	github.com text/html	MISC github.com/convos-chat/convos/commit/86b2193de375005ba71d9dd53843562c6ac1847c
Stored XSS in convos-chat/convos	blog.pocas.kr text/html	MISC blog.pocas.kr/2021/12/30/2021-12-30-s-xss-convos-chat/#Second-vulnerability
Stored XSS via attribute · Advisory · convos-chat/convos · GitHub	github.com text/html	CONFIRM github.com/convos-chat/convos/security/advisories/GHSA-xmpj-xwm3-vww7
Cross-site Scripting (XSS) - Stored vulnerability found in convos	www.huntr.dev text/html	MISC www.huntr.dev/bounties/4532a0ac-4e7c-4fcf-9fe3-630e132325c0/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, 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	Convos	Convos	All	All	All	All

cpe:2.3:a:convos:convos:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-21649 : Convos is an open source multi-user chat that runs in a web browser. Characters starting with "htt… twitter.com/i/web/status/1…	2022-01-04 20:53:54
/r/netcve	CVE-2022-21649	2022-01-04 21:38:21

← Previous ID Next ID→

CVE.report and Source URL Uptime Status status.cve.report