

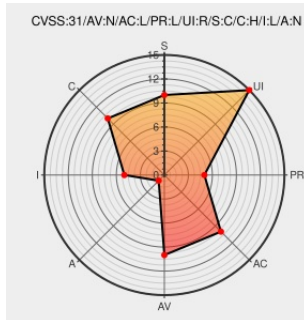


CVE-2022-21650

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

Last Modified on: 01/11/2022 09:48:00 PM UTC

CVE-2022-21650 - advisory for GHSA-mm2v-4v7g-m695

[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. You can't use SVG extension in Convos' chat window, but you can upload a file with an .html extension. By uploading an SVG file with an html extension the upload filter can be bypassed. This causes Stored XSS. Also, after uploading a file the XSS attack is triggered upon a user viewing the file. Through this vulnerability, an attacker is capable to execute malicious scripts. Users are advised to update as soon as possible.

CVE-2022-21650 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [convos-chat](#) - **convos** version ≥ 6.48 , < 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				
Cross-site Scripting (XSS) - Stored vulnerability found in convos	www.huntr.dev text/html	MISC www.huntr.dev/bounties/ae424798-de01-4972-b73b-2db674f82368/				
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/#First-vulnerability				
Add more rules for files with Content-Disposition · convos-chat/convos@5c0a1ec · GitHub	github.com text/html	MISC github.com/convos-chat/convos/commit/5c0a1ec9a2c147bc3b63fd5a48da5f32e18fe5df				
Stored XSS via html file upload · Advisory · convos-chat/convos · GitHub	github.com text/html	CONFIRM github.com/convos-chat/convos/security/advisories/GHSA-mm2v-4v7g-m695				
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-2022-21650 : Convos is an open source multi-user chat that runs in a web browser. You can't use SVG extension i... twitter.com/i/web/status/1...					2022-01-04 20:49:04
/r/netcve	CVE-2022-21650					2022-01-04 21:38:19
← Previous ID			Next ID →			

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)