



CVE-2023-37259

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-37259
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-07-18 17:15:00 UTC
Updated	2023-07-27 19:50:00 UTC
Description	matrix-react-sdk is a react-based SDK for inserting a Matrix chat/voip client into a web page. The Export Chat feature includ

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Matrix-react-sdk Project	Matrix-react-sdk	All	All	All	All
Application	Matrix-react-sdk Project	Matrix-react-sdk	3.76.0	rc1	All	All
Application	Matrix-react-sdk Project	Matrix-react-sdk	3.76.0	rc2	All	All

References

Reference	Source	Link	Ta
Sanitise strings going into the html export CVE-2023-37259 · matrix-org/matrix-react-sdk@22fcd34 · GitHub	MISC	github.com	
Potential for XSS in Export Chat feature · Advisory · matrix-org/matrix-react-sdk · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[691214](#) Free Berkeley Software Distribution (FreeBSD) Security Update for element (c70c3dc3-258c-11ee-b37b-901b0e9408dc)

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)