



CVE-2023-30609

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

Summary

CVE	CVE-2023-30609
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-25 21:15:00 UTC
Updated	2023-05-08 18:05:00 UTC
Description	matrix-react-sdk is a react-based SDK for inserting a Matrix chat/VoIP client into a web page. Prior to version 3.71.0, plain t

Risk And Classification

Problem Types: CWE-74

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

References

Reference	Source	Link
HTML injection in search results via plaintext message highlighting · Advisory · matrix-org/matrix-react-sdk · GitHub	MISC	github.com
Merge pull request from GHSA-xv83-x443-7rmw · matrix-org/matrix-react-sdk@bf182bc · GitHub	MISC	github.com
Release v3.71.0 · matrix-org/matrix-react-sdk · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.c
NVD vulnerability detail	NVD	nvd.nist.gc

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

502990 Alpine Linux Security Update for riot-web

503175 Alpine Linux Security Update for element-web

506035 Alpine Linux Security Update for element-web

© [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](#)