



CVE-2023-26140

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2023-26140
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-16 05:15:00 UTC
Updated	2023-11-07 04:09:00 UTC
Description	Versions of the package @excalidraw/excalidraw from 0.0.0 are vulnerable to Cross-site Scripting (XSS) via embedded link

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Excalidraw	Excalidraw	All	All	All	All

References

Reference	Source	Link	Ta
fix: stronger enforcement of normalizeLink (#6728) · excalidraw/excalidraw@b33fa6d · GitHub	MISC	github.com	
Cross-site Scripting (XSS) in @excalidraw/excalidraw CVE-2023-26140 Snyk	MISC	security.snyk.io	
fix: stronger enforcement of normalizeLink by vjeux · Pull Request #6728 · excalidraw/excalidraw · 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

[994885](#) NodeJs (Npm) Security Update for @excalidraw/excalidraw (GHSA-v7v8-gjv7-ffmr)

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