



CVE-2022-25875

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

Summary

CVE	CVE-2022-25875
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-07-12 19:15:00 UTC
Updated	2022-07-19 02:23:00 UTC
Description	The package svelte before 3.49.0 are vulnerable to Cross-site Scripting (XSS) due to improper input sanitization and to imp

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
github.com/sveltejs/svelte/pull/7530%23issuecomment-1158575990	MISC	github.com	
Cross-site Scripting (XSS) in svelte CVE-2022-25875 Snyk	MISC	snyk.io	
[fix] harden attribute escaping during ssr (#7530) · sveltejs/svelte@f8605d6 · GitHub	MISC	github.com	
[fix] harden attribute escaping during ssr by mrkishi · Pull Request #7530 · sveltejs/svelte · GitHub	MITRE	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, au

Vendor Comments And Credit

Discovery Credit

LEGACY: Maurício Kishi

There are currently no legacy QID mappings associated with this CVE.

© [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](#)