



CVE-2022-25929

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

Summary

CVE	CVE-2022-25929
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-12-21 05:15:00 UTC
Updated	2022-12-27 22:43:00 UTC
Description	The package smoothie from 1.31.0 and before 1.36.1 are vulnerable to Cross-site Scripting (XSS) due to improper user inp

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Smoothiecharts	Smoothie Charts	All	All	All	All

References

Reference
fix: potential XSS when `tooltipLabel` or `strokeStyle` are controle... · joewalnes/smoothie@8e0920d · GitHub
fix: potential XSS when `tooltipLabel` or `strokeStyle` are controlled by users by WofWca · Pull Request #147 · joewalnes/smoothie · GitHub
Cross-site Scripting (XSS) in org.webjars.bower:smoothie CVE-2022-25929 Snyk
Cross-site Scripting (XSS) in smoothie CVE-2022-25929 Snyk
Cross-site Scripting (XSS) in org.webjars:smoothie CVE-2022-25929 Snyk
CVE Program record
NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit
LEGACY: WofWca

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](#)