



CVE-2022-21169

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

Summary

CVE	CVE-2022-21169
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-26 05:15:00 UTC
Updated	2022-09-28 17:21:00 UTC
Description	The package express-xss-sanitizer before 1.1.3 are vulnerable to Prototype Pollution via the allowedTags attribute, allowing

Risk And Classification

Problem Types: CWE-1321

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Express Xss Sanitizer Project	Express Xss Sanitizer	All	All	All	All

References

Reference	Source	Link
XSS bypass by using prototype pollution · Issue #4 · AhmedAdelFahim/express-xss-sanitizer · GitHub	CONFIRM	github.com
Prototype Pollution in express-xss-sanitizer CVE-2022-21169 Snyk	CONFIRM	security.snyk.io
fix XSS bypass by using prototype pollution issue. · AhmedAdelFahim/express-xss-sanitizer@3bf8aaa · GitHub	CONFIRM	github.com
RunKit	CONFIRM	runkit.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Jayateertha Guruprasad

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](#)