



CVE-2021-29624

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

Summary

CVE	CVE-2021-29624
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-19 22:15:00 UTC
Updated	2022-10-25 20:56:00 UTC
Description	fastify-csrf is an open-source plugin helps developers protect their Fastify server against CSRF attacks. Versions of fastify-c

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fastify	Fastify-csrf	All	All	All	All

References

Reference	Source	Link
Release v3.1.0 · fastify/fastify-csrf · GitHub	MISC	github.com
Cross-Site Request Forgery Prevention - OWASP Cheat Sheet Series	MISC	cheatsheetseries.c
Add utilities to prevent cookie tossing and replay attacks by mcollina · Pull Request #2 · fastify/csrf · GitHub	MISC	github.com
Lack of protection against cookie tossing attacks in fastify-csrf · Advisory · fastify/fastify-csrf · GitHub	CONFIRM	github.com
Support userInfo by mcollina · Pull Request #51 · fastify/fastify-csrf · GitHub	MISC	github.com
owasp.org/www-pdf-archive/David_Johansson-Double_Defeat_of_Double-Submi...	MISC	owasp.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

982378 Nodejs (npm) Security Update for @fastify/csrf (GHSA-rc4q-9m69-gqp8)

© [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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)