CVE-2023-31999

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2023-31999
State	PUBLIC
Assigner	support@hackerone.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-07-04 17:15:00 UTC
Updated	2023-07-17 18:49:00 UTC
Description	All versions of @fastify/oauth2 used a statically generated state parameter at startup time and were used across all request

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fastify	Oauth2	All	All	All	All

References

Reference	Source	Link	Tags
Release v7.2.0 · fastify/fastify-oauth2 · GitHub	MISC	github.com	
HackerOne	MISC	hackerone.com	
Prevent Attacks and Redirect Users with OAuth 2.0 State Parameters	MISC	auth0.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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