CVE-2022-29035

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

Summary

CVE	CVE-2022-29035
State	PUBLIC
Assigner	security@jetbrains.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-11 19:15:00 UTC
Updated	2022-04-15 17:46:00 UTC
Description	In JetBrains Ktor Native before version 2.0.0 random values used for nonce generation weren't using SecureRandom imple

Risk And Classification

Problem Types: CWE-330

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jetbrains	Ktor	All	All	All	All

References

Reference	Source	Link
KTOR-3656 Use secure random for nonce generation by rsinukov · Pull Request #2776 · ktorio/ktor · GitHub	MISC	github.com
Fixed security issues	MISC	www.jetbrains.cor
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Dan Wallach

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report