CVE-2021-4239

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

Summary

CVE	CVE-2021-4239
State	PUBLIC
Assigner	security@golang.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-12-27 22:15:00 UTC
Updated	2023-01-06 01:30:00 UTC
Description	The Noise protocol implementation suffers from weakened cryptographic security after encrypting 2^64 messages, and a p

Risk And Classification

Problem Types: CWE-311

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Noiseprotocol	Noise	-	All	All	All

References

Reference	Source	Link	Tags
GO-2022-0425 - Go Packages	MISC	pkg.go.dev	
Fix nonce handling by titanous · Pull Request #44 · flynn/noise · GitHub	MISC	github.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.

Free CVE JSON API cve.report/api

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