CVE-2022-48570

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-48570
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-22 19:16:00 UTC
Updated	2023-08-26 02:21:00 UTC
Description	Crypto++ through 8.4 contains a timing side channel in ECDSA signature generation. Function FixedSizeAllocatorWithClea

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cryptopp	Crypto	All	All	All	All

References

Reference	Source	Link	Tags
AppVeyor failures after fixing FixedSizeSecBlock · Issue #992 · weidai11/cryptopp · GitHub	MISC	github.com	
Release Crypto++ 8.4 release · weidai11/cryptopp · 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.

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