CVE-2021-43398

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-43398
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-11-04 21:15:00 UTC
Updated	2023-11-07 03:39:00 UTC
Description	** DISPUTED ** Crypto++ (aka Cryptopp) 8.6.0 and earlier contains a timing leakage in MakePublicKey(). There is a clear c

Risk And Classification

Problem Types: CWE-203

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	T
Dangerous Correlation Between Key Length and Execution Time · Issue #1080 · weidai11/cryptopp · GitHub	MISC	github.com	
Dangerous Correlation Between Key Length and Execution Time · Issue #1080 · weidai11/cryptopp · GitHub	MISC	github.com	
Crypto++ Library 8.6 | Free C++ Class Library of Cryptographic Schemes	MISC	cryptopp.com	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

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