



# CVE-2021-43398

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#) 

## Summary

<b>CVE</b>	CVE-2021-43398
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-11-04 21:15:00 UTC
<b>Updated</b>	2023-11-07 03:39:00 UTC
<b>Description</b>	** DISPUTED ** Cryptopp (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	<a href="#">Cryptopp</a>	<a href="#">Crypto</a>	All	All	All	All

## References

Reference	Source	Link	Ti
Dangerous Correlation Between Key Length and Execution Time · Issue #1080 · weidai11/cryptopp · GitHub	MISC	<a href="#">github.com</a>	
Dangerous Correlation Between Key Length and Execution Time · Issue #1080 · weidai11/cryptopp · GitHub	MISC	<a href="#">github.com</a>	
Cryptopp Library 8.6   Free C++ Class Library of Cryptographic Schemes	MISC	<a href="#">cryptopp.com</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	ca
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	ca

No vendor comments have been submitted for this CVE.

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

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered 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](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**