CVE-2022-29566

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-29566
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-21 19:15:00 UTC
Updated	2023-08-08 14:22:00 UTC
Description	The Bulletproofs 2017/1066 paper mishandles Fiat-Shamir generation because the hash computation fails to include all of t

Risk And Classification

Problem Types: CWE-326

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bulletproofs Project	Bulletproofs	-	All	All	All

References

Reference	Source	Link
Cryptology ePrint Archive: Report 2017/1066 - Bulletproofs: Short Proofs for Confidential Transactions and More	MISC	eprint.iacr.org
Coordinated disclosure of vulnerabilities affecting Girault, Bulletproofs, and PlonK | Trail of Bits Blog	MISC	blog.trailofbits
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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