



CVE-2023-33242

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

Summary

CVE	CVE-2023-33242
State	PUBLIC
Assigner	disclosures@halborn.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-09 22:15:00 UTC
Updated	2023-08-25 15:06:00 UTC
Description	Crypto wallets implementing the Lindell17 TSS protocol might allow an attacker to extract the full ECDSA private key by exf

Risk And Classification

Problem Types: CWE-74

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lindell17 Project	Lindell17	-	All	All	All

References

Reference	Source	Link	Tags
GitHub - fireblocks-labs/zengo-lindell17-exploit-poc	MISC	github.com	
GitHub - fireblocks-labs/mpc-ecdsa-attacks-23	MISC	github.com	
Lindell17 Abort Vulnerability [CVE-2023-33242]: Technical Report - Fireblocks	MISC	www.fireblocks.com	
eprint.iacr.org/2017/552.pdf	MISC	eprint.iacr.org	
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.

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#).

Free CVE JSON API cve.report/api

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