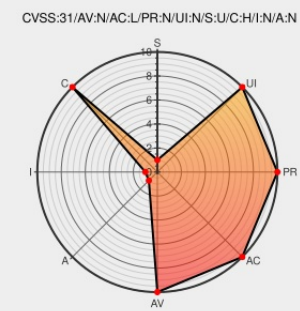
CVE-2023-26557

Published on: Not Yet Published

Last Modified on: 05/02/2023 05:06:00 PM UTC

CVE-2023-26557

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Tss-lib from Iofinnet contain the following vulnerability:

io.finnet tss-lib before 2.0.0 can leak the lambda value of a private key via a timing side-channel attack because it relies on Go big.Int, which is not constant time for Cmp, modular exponentiation, or modular inverse. An example leak is in crypto/paillier/paillier.go. (bnb-chain/tss-lib and thorchain/tss are also affected.)

CVE-2023-26557 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	NONE

CVE References

Description	Tags	Link
GitHub - bnb-chain/tss-lib at v1.3.5	github.com text/html	MISC github.com/bnb-chain/tss-lib/tree/v1.3.5
Release v2.0.0 · IoFinnet/tss-lib · GitHub	github.com text/html	MISC github.com/IoFinnet/tss-lib/releases/tag/v2.0.0
v0.1.3 · Tags · THORChain / THORChain TSS / tss-lib · GitLab	gitlab.com text/html	MISC gitlab.com/thorchain/tss/tss-lib/-/tags/v0.1.3
Security disclosure for ECDSA and EdDSA threshold signature schemes | by io.finnet | Mar, 2023 | Medium	medium.com text/html	MISC medium.com/@iofinnet/security-disclosure-for-ecdsa-and-eddsa-threshold-signature-schemes-4e969af7155b

are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Iofinnet	Tss-lib	All	All	All	All

cpe:2.3:a:iofinnet:tss-lib:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-26557 : io.finnet tss-lib before 2.0.0 can leak the lambda value of a private key via a timing side-channe… twitter.com/i/web/status/1…	2023-04-21 18:06:29

← Previous ID

Next ID→