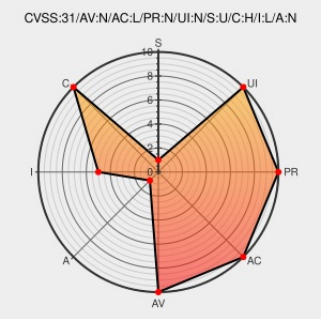
CVE-2020-12118

Published on: 04/23/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:35 PM UTC

CVE-2020-12118

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



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

The keygen protocol implementation in Binance tss-lib before 1.2.0 allows attackers to generate crafted h1 and h2 parameters in order to compromise a signing round or obtain sensitive information from other parties.

CVE-2020-12118 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.2 - HIGH

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

CVSS2 Score: 6.4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
keygen dlnproof by notatestuser · Pull Request #89 · binance-chain/tss-lib · GitHub	Patch, Third Party Advisory, github.com, text/html	MISC github.com/binance-chain/tss-lib/pull/89

Release Various bug fixes · binance-chain/tss-lib · GitHub	Release Notes Third Party Advisory github.com text/html	MISC github.com/binance-chain/tss-lib/releases/tag/v1.2.0

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that 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.

Related QID Numbers

982032 Go (go) Security Update for github.com/binance-chain/tss-lib/ecdsa/keygen (GHSA-399h-cmvp-qgx5)

Known Affected Configurations (CPE V2.3)

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

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 | |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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 registred 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