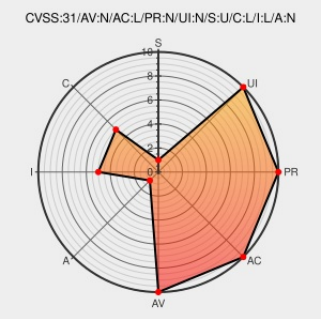
CVE-2022-23507

Published on: Not Yet Published

Last Modified on: 12/20/2022 04:14:00 PM UTC

CVE-2022-23507 - advisory for GHSA-xqqc-c5gw-c5r5

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



Certain versions of Tendermint-light-client-js from Tendermint-light-client-js Project contain the following vulnerability:

Tendermint is a high-performance blockchain consensus engine for Byzantine fault tolerant applications. Versions prior to 0.28.0 contain a potential attack via Improper Verification of Cryptographic Signature, affecting anyone using the tendermint-light-client and related packages to perform light client verification (e.g. IBC-rs, Hermes). The light client does not check that the chain IDs of the trusted and untrusted headers match, resulting in a possible attack vector where someone who finds a header from an untrusted chain that satisfies all other verification conditions (e.g. enough overlapping validator signatures) could fool a light client. The attack vector is currently theoretical, and no proof-of-concept exists yet to exploit it on live networks. This issue is patched in version 0.28.0. There are no workarounds.

CVE-2022-23507 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **informalsystems** - **tendermint-rs** version **= 0.28.0**

CVSS3 Score: 6.5 - MEDIUM

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

CVE References

Description	Tags	Link
Light client verification not taking into account chain ID · Advisory · informalsystems/tendermint-rs · GitHub	github.com text/html	MISC github.com/informalsystems/tendermint-rs/security/advisories/GHSA-xqqc-c5gw-c5r5

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tendermint-light-client-js Project	Tendermint-light-client-js	All	All	All	All
Application	Tendermint-light-client-verifier Project	Tendermint-light-client-verifier	All	All	All	All
Application	Tendermint-light-client Project	Tendermint-light-client	All	All	All	All

cpe:2.3:a:tendermint-light-client-js_project:tendermint-light-client-js:*:*:*:*:rust:*:*:*:

cpe:2.3:a:tendermint-light-client-verifier_project:tendermint-light-client-verifier:*:*:*:*:*:rust:*:*:

cpe:2.3:a:tendermint-light-client_project:tendermint-light-client:*:*:*:*:rust:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→