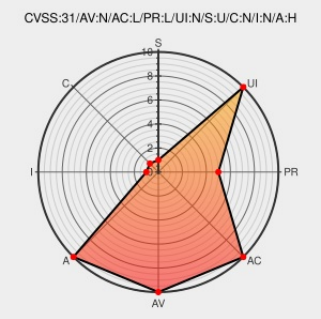
CVE-2021-21271

Published on: 01/26/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:59 PM UTC

CVE-2021-21271 - advisory for GHSA-p658-8693-mhvg

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



Certain versions of Tendermint from Tendermint contain the following vulnerability:

Tendermint Core is an open source Byzantine Fault Tolerant (BFT) middleware that takes a state transition machine - written in any programming language - and securely replicates it on many machines. Tendermint Core v0.34.0 introduced a new way of handling evidence of misbehavior. As part of this, we added a new Timestamp field to Evidence structs. This timestamp would be calculated using the same algorithm that is used when a block is created and proposed. (This algorithm relies on the timestamp of the last commit from this specific block.) In Tendermint Core v0.34.0-v0.34.2, the consensus reactor is responsible for forming DuplicateVoteEvidence whenever double signs are observed. However, the current block is still “in flight” when it is being formed by the consensus reactor. It hasn’t been finalized through network consensus yet. This means that different nodes in the network may observe different “last commits” when assigning a timestamp to DuplicateVoteEvidence. In turn, different nodes could form DuplicateVoteEvidence objects at the same height but with different timestamps. One DuplicateVoteEvidence object (with one timestamp) will then eventually get finalized in the block, but this means that any DuplicateVoteEvidence with a different timestamp is considered invalid. Any node that formed invalid DuplicateVoteEvidence will continue to propose invalid evidence; its peers may see this, and choose to disconnect from this node. This bug means that double signs are DoS vectors in Tendermint Core v0.34.0-v0.34.2. Tendermint Core v0.34.3 is a security release which fixes this bug. As of v0.34.3, DuplicateVoteEvidence is no longer formed by the consensus reactor; rather, the consensus reactor passes the Votes themselves into the EvidencePool, which is now responsible for forming DuplicateVoteEvidence. The EvidencePool has timestamp info that should be consistent across the network, which means that DuplicateVoteEvidence formed in this reactor should have consistent timestamps. This release changes the API between the consensus and evidence reactors.

CVE-2021-21271 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **tendermint** - **tendermint** version **>= 0.34.0, < 0.34.3**

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
Security Advisory Mulberry · Advisory · tendermint/tendermint · GitHub	Third Party Advisory, github.com, text/html	CONFIRM github.com/tendermint/tendermint/security/advisories/GHSA-p658-869 mhvg
use correct source of evidence time · tendermint/tendermint@a2a6852 · GitHub	Patch, Third Party Advisory, github.com, text/html	MISC github.com/tendermint/tendermint/commit/a2a6852ab99e4a0f9e79f0ea8c1726e262e
tendermint/CHANGELOG.md at v0.34.3 · tendermint/tendermint · GitHub	Release Notes, Third Party Advisory, github.com, text/html	MISC github.com/tendermint/tendermint/blob/v0.34.3/CHANGELOG.md#v0.34.3

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tendermint	Tendermint	All	All	All	All

cpe:2.3:a:tendermint:tendermint:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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