Security Advisory Syringa

Moderate **melekes** published **GHSA-6jqj-f58p-mrw3** on Jul 2, 2020

Package

No package listed

Affected versions

>= v0.33.0

Patched versions

v0.33.6

Description

Description

Denial of Service

Tendermint 0.33.0 and above allow block proposers to include signatures for the wrong block. This may happen naturally if you start a network, have it run for some time and restart it without changing the chainID. (It is a misconfiguration to reuse chainIDs.) Correct block proposers will accidentally include signatures for the wrong block if they see these signatures, and then commits won't validate, making all proposed blocks invalid. A malicious validator (even with a minimal amount of stake) can use this vulnerability to completely halt the network.

Tendermint 0.33.6 checks all the signatures are for the block with +2/3 majority before creating a commit.

False Witness

Tendermint 0.33.1 and above are no longer fully verifying commit signatures during block execution - they stop after +2/3. This means proposers can propose blocks that contain valid +2/3 signatures and then the rest of the signatures can be whatever they want. They can claim that all the other validators signed just by including a CommitSig with arbitrary signature data. While this doesn't seem to impact safety of Tendermint per se, it means that Commits may contain a lot of invalid data **.

** *This was already true of blocks, since they could include invalid txs filled with garbage, but in that case the application knew that they are invalid and could punish the proposer. But since applications didn't--and don't-- verify commit signatures directly (they trust Tendermint to do that), they won't be able to detect it.*

This can impact incentivization logic in the application that depends on the LastCommitInfo sent in BeginBlock, which includes which validators signed. For instance, Gaia incentivizes proposers with a bonus for including more than +2/3 of the signatures. But a proposer can now claim that bonus just by including arbitrary data for the final -1/3 of validators without actually waiting for their signatures. There may be other tricks that can be played because of this.

Tendermint 0.33.6 verifies all the signatures during block execution ***.

*** *Please note that the light client does not check nil votes and exits as soon as 2/3+ of the signatures are checked.*

Impact

- All nodes
- The network stops due to having a commit with a wrong signature.

Patches

- v0.33.6

Workarounds

No workarounds.

References

- #4926

For more information

If you have any questions or comments about this advisory:

- Open an issue in tendermint/tendermint
- Email us at security@tendermint.com

More information can be found here.

Severity

Moderate

CVE ID

CVE-2020-15091

Weaknesses

No CWEs

Credits

ebuchman

melekes