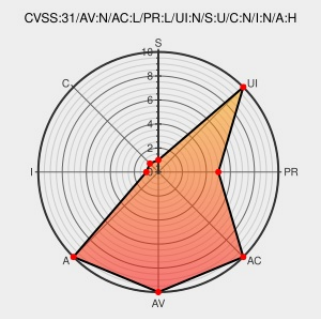
CVE-2020-15091

Published on: 07/02/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:41 PM UTC

CVE-2020-15091 - advisory for GHSA-6jqj-f58p-mrw3

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



Certain versions of Tendermint from Tendermint contain the following vulnerability:

TenderMint from version 0.33.0 and before version 0.33.6 allows 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 chainID**). A malicious block proposer (even with a minimal amount of stake) can use this vulnerability to completely halt the network. This issue is fixed in Tendermint 0.33.6 which checks all the signatures are for the block with 2/3+ majority before creating a commit.

CVE-2020-15091 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **tendermint** - **tendermint** version **>= 0.33.0, < 0.33.6**

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
consensus: Do not allow signatures for a wrong block in commits · tendermint/tendermint@480b995 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/tendermint/tendermint/commit/480b995a31727593f58b361af979054d17
Consensus: "enterPrevote: ProposalBlock is invalid" - Error: "wrong signature" · Issue #4926 · tendermint/tendermint · GitHub	Exploit Issue Tracking Third Party Advisory github.com text/html	MISC github.com/tendermint/tendermint/issues/4926
Security Advisory Syringa · Advisory · tendermint/tendermint · GitHub	Exploit Third Party Advisory github.com text/html	CONFIRM github.com/tendermint/tendermint/security/advisories/GHSA-6jqj-f58p-

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
Application	Tendermint	Tendermint	All	All	All	All

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→