

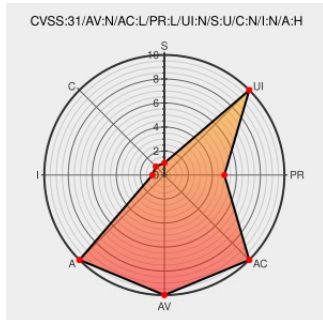


CVE-2020-15091

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 $\geq 0.33.0$, $< 0.33.6$

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

consensus: Do not allow signatures for a wrong block in commits · tendermint/tendermint@480b995 · GitHub

Tags

Patch

Third Party Advisory

github.com

text/html

Link

MISC

github.com/tendermint/tendermint/commit/480b995a31727593f58b361af979054d17c

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

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	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 →

© 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 registered 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](#)