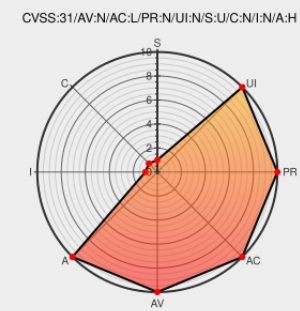
CVE-2019-25072

Published on: Not Yet Published

Last Modified on: 02/28/2023 06:07:18 PM UTC

CVE-2019-25072

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



Certain versions of Tendermint from Tendermint contain the following vulnerability:

Due to support of Gzip compression in request bodies, as well as a lack of limiting response body sizes, a malicious server can cause a client to consume a significant amount of system resources, which may be used as a denial of service vector.

CVE-2019-25072 has been assigned by security@golang.org to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **github.com/tendermint/tendermint** - **github.com/tendermint/tendermint/rpc/lib/client** version **< 0.31.1**

CVSS3 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
rpc: client disable compression (#3430) · tendermint/tendermint@03085c2 · GitHub	github.com text/html	MISC github.com/tendermint/tendermint/commit/03085c2da23b179c4a51f59a03cb40aa4e85a613
rpc: client disable compression by guagualvcha · Pull Request #3430 · tendermint/tendermint · GitHub	github.com text/html	MISC github.com/tendermint/tendermint/pull/3430
GO-2020-0037 - Go Packages	pkg.go.dev text/html	MISC pkg.go.dev/vuln/GO-2020-0037

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

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