



CVE-2022-29219

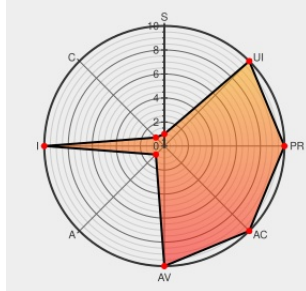
Published on: Not Yet Published

Last Modified on: 06/07/2022 04:25:00 PM UTC

CVE-2022-29219 - advisory for GHSA-cvj7-5f3c-9vg9

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N



Certain versions of [Lodestar](#) from [Chainsafe](#) contain the following vulnerability:

Lodestar is a TypeScript implementation of the Ethereum Consensus specification. Prior to version 0.36.0, there is a possible consensus split given maliciously-crafted `AttesterSlashing` or `ProposerSlashing` being included on-chain. Because the developers represent `uint64` values as native javascript `number`s, there is an issue when those

variables with large (greater than 2^{53}) `uint64` values are included on chain. In those cases, Lodestar may view valid `AttesterSlashing` or `ProposerSlashing` as invalid, due to rounding errors in large `number` values. This causes a consensus split, where Lodestar nodes are forked away from the main network. Similarly, Lodestar may consider invalid `ProposerSlashing` as valid, thus including in proposed blocks that will be considered invalid by the network. Version 0.36.0 contains a fix for this issue. As a workaround, use `BigInt` to represent `Slot` and `Epoch` values in `AttesterSlashing` and `ProposerSlashing` objects. `BigInt` is too slow to be used in all `Slot` and `Epoch` cases, so one may carefully use `BigInt` just where necessary for consensus.

CVE-2022-29219 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [ChainSafe](#) - **lodestar** version < 0.36.0

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	HIGH	NONE

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
---------------	-------------------	----------------

CONFIDENTIALITY	INTEGRITY	AVAILABILITY
Network	Low	None
Confidentiality Impact	Integrity Impact	Availability Impact
None	Partial	None

CVE References

Description	Tags	Link
Release Release v0.36.0 · ChainSafe/lodestar · GitHub	github.com text/html	 MISC github.com/ChainSafe/lodestar/releases/tag/v0.36.0
AttesterSlashing number overflow · Advisory · ChainSafe/lodestar · GitHub	github.com text/html	 CONFIRM github.com/ChainSafe/lodestar/security/advisories/GHSA-cvj7-5f3c-9vg9
Reorg uint variables by dapplion · Pull Request #3977 · ChainSafe/lodestar · GitHub	github.com text/html	 MISC github.com/ChainSafe/lodestar/pull/3977

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	Chainsafe	Lodestar	All	All	All	All

cpe:2.3:a:chainsafe:lodestar:*.*.*.*.*.*.*.*.:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-29219 : Lodestar is a TypeScript implementation of the Ethereum Consensus specification. Prior to version... twitter.com/i/web/status/1...	2022-05-24 14:31:35
 /r/netcve	CVE-2022-29219	2022-05-24 15:38:15

[← Previous ID](#)

Next ID→

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](#)