

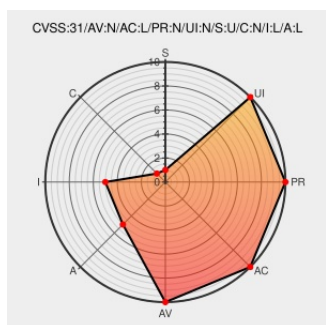


CVE-2022-46173

Published on: Not Yet Published

Last Modified on: 01/09/2023 02:17:00 PM UTC

CVE-2022-46173 - advisory for GHSA-p228-4mrh-ww7r

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

Certain versions of [Elrond Go](#) from [Elrond](#) contain the following vulnerability:

Elrond-GO is a go implementation for the Elrond Network protocol. Versions prior to 1.3.50 are subject to a processing issue where nodes are affected when trying to process a cross-shard relayed transaction with a smart contract deploy transaction data. The problem was a bad correlation between the transaction caches and the processing

component. If the above-mentioned transaction was sent with more gas than required, the smart contract result (SCR transaction) that should have returned the leftover gas, would have been wrongly added to a cache that the processing unit did not consider. The node stopped notarizing metachain blocks. The fix was actually to extend the SCR transaction search in all other caches if it wasn't found in the correct (expected) sharded-cache. There are no known workarounds at this time. This issue has been patched in version 1.3.50.

CVE-2022-46173 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [ElrondNetwork](#) - **elrond-go** version = < 1.3.50

CVSS3 Score: **6.5 - MEDIUM**

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

CVE References

Description	Tags	Link
Improve SCR lookup in smartcontract preprocessor by iulianpascalau · Pull Request #4718 · ElrondNetwork/elrond-go	github.com text/html	MISC github.com/ElrondNetwork/elrond-go/pull/4718

Merge pull request #4718 from ElrondNetwork/test-scr-processor-lookup · ElrondNetwork/elrond-go@39d7ddc · GitHub

[github.com](#)
[text/html](#)

 MISC [github.com/ElrondNetwork/elrond-go/commit/39d7ddcb08bb34217dab6daef7cd9d287fb8cab3](#)

Processing: fallback search of SCRs when not found in the main cache · Advisory · ElrondNetwork/elrond-go · GitHub

[github.com](#)
[text/html](#)

 MISC [github.com/ElrondNetwork/elrond-go/security/advisories/GHSA-p228-4mrh-ww7r](#)

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

Exploit/POC from Github

Elrond-GO is a go implementation for the Elrond Network protocol. Versions prior to 1.3.50 are subject to a processin...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Elrond	Elrond Go	All	All	All	All
cpe:2.3:a:elrond:elrond_go:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-46173 : Elrond-GO is a go implementation for the Elrond Network protocol. Versions prior to 1.3.50 are sub... twitter.com/i/web/status/1...	2022-12-28 07:08:41
 /r/netcve	CVE-2022-46173	2022-12-28 08:38:41

[← Previous ID](#)

[Next ID →](#)