Flare Songbird

Security Review Update: May 15, 2024

Reviewer: balthasar@gofyeo.com

May 2024
Version 1.0

Presented by:
FYEO Inc.
PO Box 147044
Lakewood CO 80214
United States

Security Level
Public

Flare Security Review Update

New security issues, 1 (Informational)

After the development team implemented the latest updates, FYEO conducted a review of the modifications. The primary goal of this evaluation was to ensure the continued robustness of the network's security features, safeguarding the network's integrity and maintaining the overall robustness of the codebase.

General Updates:

The reviewed update brings several enhancements to the Flare codebase, with the primary objective of integrating Songbird and Coston (its test network). These changes encompass the integration of genesis data, staking weights, block times, validators, fork dates, and gas limits, among others.

Furthermore, the submitter contract logic has been consolidated into IsPrioritisedContractCall, with the state transition logic dynamically adjusting its behavior based on the network it operates on, whether Songbird or otherwise.

An addition is the support for default validator sets loaded during VM initialization, used by the Songbird/Coston networks to incorporate validators with low weights. Additionally, the implementation includes the introduction of a NetworkValue data structure, facilitating the storage of network-specific data such as inflation settings tied to their respective network IDs.

In alignment with network transitions, export and import transactions for Songbird have been disabled prior to the designated transition time, ensuring seamless network operation.

Moreover, these updates encompass robust testing, with a comprehensive suite of tests validating the accurate implementation of these modifications. Support for local testnets for both networks has been integrated, providing testing environments for developers on either network.

Commit Hash Reference:

For transparency and reference, the security review was conducted on a specific commit hash. The commit hash for the reviewed version is as follows:

4b86b5cbd8beaf164324b1f84635ff04cccb201b

Conclusion:

In conclusion, the security aspects of the Flare network remain robust and unaffected by the recent updates. Users can confidently interact with the network, assured that their assets are well-protected. The commitment to security exhibited by the development team is commendable, and we appreciate the ongoing efforts to prioritize the safeguarding of network users.

Typo in defaultValidatorSet

Finding ID: FYEO-FLARE-01
Severity: **Informational**
Status: **Remediated**

Description

There is a typo in the variable initialzed.

Proof of Issue

File name: avalanchego/snow/validators/custom.go
Line number: 40

```
type defaultValidatorSet struct {
    initialzed bool
    vdrMap     map[ids.NodeID]Validator
}
```

Severity and Impact Summary

No security impact.

Recommendation

Rename initialzed to initialized.