Flare Songbird

Security Review Update: June 20, 2024

Reviewer: balthasar@gofyeo.com

June 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, 0

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 Flare project has undergone several changes to upgrade it to Avalanche version 1.9.0 and Coreth v0.11.0. The network configuration settings, and configurations for Songbird, Flare and their test networks have been updated. An application prefix has been set specifically for Songbird ("flare") and Flare ("avalanche") using the InitApplicationPrefix function. In the vms/platformvm/reward/calculator.go, the reward calculation function was simplified to always return zero - this is because these are instead handled in smart contracts. Changes were also made indicating that Flare / Songbird do not allow the creation of subnets or adding permissionless validator transactions. For validators, the DefaultValidatorList and defaultValidatorSet were added, along with proper tests. These validators have a limited validity.

Core Ethereum adjustments included updates to block rate and gas limit settings and setting the NativeAssetCallDeprecationTime to September 16, 2022. Improvements were made in handling attestation votes to ensure error management and correct plurality assignment, including logic for handling discrepancies in attestation decisions and potential node forking. In the state transition, Flare and Songbird specific handling was added in core/state_transition.go, with adjustments based on chain ID and timestamp, and checks for prioritized contract calls. Finally, local Flare chain configuration and Songbird local network configurations were defined.

To address concerns with inter-chain fund transfers, the gas limit for the Songbird chain was reduced to 8 million to align with Avalanche defaults and prevent potential issues. These changes were implemented with commit hash 7a3db361a9933d33244bd09a666e708fdee6cf91.

These changes collectively advance the code base by integrating updates from a more recent version of Avalanche.

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:

Flare: 7a3db361a9933d33244bd09a666e708fdee6cf91
Coreth: 4732e0b513ac338922eee932aee36afc47519eeb

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.