Flare Songbird

Security Review Update: March 10, 2025

Reviewer: balthasar@gofyeo.com

March 2025
Version 1.0

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

Security Level
Public

Flare Security Review Update

The issue identified is with transferring funds from the C-chain to the X-chain. Although the export transaction from the C-chain works fine, the subsequent import transaction on the X-chain fails with an ‘incompatible feature extension’ error.

The X-chain verifies that an asset’s creation transaction (`CreateAssetTx`) includes a state that corresponds to the feature extension (`fxID`). This is done by checking the `States` list in the transaction.

For the default AVAX asset on the X-chain, the `States` list is empty. This is because, in the chain’s genesis configuration, no funds were assigned to any address. When the verification function runs, it does not find any state with the required `fxID`, and thus it returns an error.

Analysis of the proposed solution

For the default AVAX asset on the X-chain, the genesis configuration provided an allocation with an initial amount of 0. Since no funds were actually assigned to any address, no state entry was created in its CreateAssetTx. As a result, the States list is empty and there is no FxIndex value present. When the verifyFxUsage function later checks for a state with a matching FxIndex, it fails with an 'errIncompatibleFx' error.

The update adds a specific exception for the default AVAX asset. It is a targeted fix for a genesis configuration issue and will not impact other operations on the blockchain.

The fix (which will take effect after the 'Cortina' update) is to modify the verifyFxUsage function. This change allows the use of feature extension fxID 0 for the AVAX asset even when the States list is empty. This bypasses the errIncompatibleFx error that otherwise arises.

All other assets and operations continue to undergo the usual feature extension verification. Thus, the update does not affect any other operations on the blockchain outside of this specific scenario.

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:

c532246687b8a56603fa9dc7949b2d0bc08a7efc

Conclusion:

The implemented changes effectively mitigate the issue of the feature extension not being found and transactions failing when transferring funds from the C-chain to the X-chain.