LunaFi v1 contracts
Addressing Audit Comments

Test Coverage: Increased test coverage for all contracts.

Documentation: Increased documentation for all contracts.

Addressing Notices

1. The repository contains contracts that are out of the audit scope.

Fixed:
Only Phase 1 contracts are in the repository being audited. All phase 2 contracts will now be created in a new v2 repository and audited separately when phase 2 is ready for review.

2. LFIToken admin may blacklist any address, admin may burn all tokens from the blacklisted address, and it is impossible to send tokens from the blacklisted address.

Fixed:
Blacklist functionality has been removed from.
Burn functionality from LFIToken has been removed.
Burn method in claimToken.sol now checks for msg.sender and only allows burning user owned tokens.

3. Vesting beneficiaries can get vested tokens only after the managers' approval.

Fixed:
We have removed vesting contract and will not be using this hence this issue has been

addressed.

4. The staking contract implementation may be updated by the contract owner. The current audit covers only implementation from the scope.

Acknowledged:
This is acknowledged and part of the phased launch approach where features are launched in stages. Contact changes for each stage will be reviewed and audited before launch.

5. The admin of the staking contract may withdraw all liquidity tokens from the contract, including funds staked by users.

Fixed:
Ability of admin to withdraw liquidity has been removed from the contract

Addressing Findings

Critical

None

High

1. Vesting funds are not guaranteed.

Fixed:

We have removed vesting contract and will not be using this hence this issue has been addressed.

2. Staking liquidity funds safety is not guaranteed by the contract logic.

Fixed:

This was a last resort mechanism and we have removed the method in question. Hence Staking liquidity safety is now guaranteed.

3. Admin may burn users' funds.

Fixed:

LFIToken.sol: Burn method has been removed along with other ERC20Extended methods.
claimToken.sol: Admin cannot burn user’s tokens. A msg.sender require statement has been added to ensure this mechanism.

4. Admin may mint an unlimited amount of tokens.

Fixed:

A max supply cap has been added to ensure only allowed maximum can be minted.

Medium

1. Redundant function argument.

Fixed:

Recommendation has been implemented.

Low

1. Redundant use of SafeMath library.

Fixed:

Recommendation has been implemented.

2. Use of magic number.

Fixed:

We have removed vesting contract and will not be using this hence this issue has been addressed.

3. Unexpected output.

Fixed:

We have removed vesting contract and will not be using this hence this issue has been addressed.

Recommendations

LFIToken.sol: The token contract uses both AccessContraol and Ownable library. It is recommended not to mix these libraries, to avoid unexpected issues related to the role management during the development.

Fixed:

Recommendation has been implemented.