G₀ Group

Security Review of

TrueFi Lithium Release

May 2022

TrueFi Lithium Release / May 2022

Files in scope

Following solidity files:

https://github.com/trusttoken/contracts-lithium/tree/70f782b987be526d080744d312412d4742fe13f1

- AllowList.sol
- AllowListDepositStrategy.sol
- TrueMultiFarm.sol
- MultiFarmTransferStrategy.sol

Current status

All discovered issues have been fixed by the developer. There are no known issues in the relevant contracts in

https://github.com/trusttoken/contracts-lithium/tree/bb00e3e7ff92a26b1209c96f6088d0f2b9a63238

Issues

1. Stakes can be mistaken for rewards

type: incorrect implementation / severity: critical

In `TrueMultiFarm` when user adds a stake in tokens that are being paid out as rewards, this stake will be recognized as a reward by the contract and will be paid out. The same will happen if a reward token is added after it has been staked by users.

status - fixed

Issue has been fixed and is no longer present in

https://github.com/trusttoken/contracts-lithium/tree/bb00e3e7ff92a26b1209c96f6088d0f2b9a63238

2. Rewards that are not paid out due to lack of stakers will become irretrievable

type: incorrect implementation / severity: medium

There is no mechanism to rescue rewards that are collected when no stakes for the reward token are present, these rewards will be stuck in the contract.

status - fixed

Issue has been fixed and is no longer present in

https://github.com/trusttoken/contracts-lithium/tree/bb00e3e7ff92a26b1209c96f6088d0f2b9a63238

3. There should be a way to withdraw stakes without reward payout to avoid DoS by the owner

type: security / severity: medium

If owner adds a distrubutor contract that throws an error in the `distribute()` function, all user operations of the contract including stake withdrawal will be effectively blocked. There should be an emergency withdrawal function in the contract that allows users to withdraw their stake without `distribute()` being called.

status - fixed

Issue has been fixed and is no longer present in

https://github.com/trusttoken/contracts-lithium/tree/bb00e3e7ff92a26b1209c96f6088d0f2b9a63238