TechRate

Fundamenta

Smart Contract Security Audit

October, 2020

TechRate
https://techrate.org

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and TechRate and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (TechRate) owe no duty of care towards you or any other person, nor does TechRate make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and TechRate hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, TechRate hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against TechRate, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

Background

TechRate was commissioned by Fundamenta to perform an audit of smart contract:

- *LiquidityMining.sol*
- *Fundamenta.sol*
- *TokenStaking.sol*

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

High Severity Issues

1. Wrong reward calculation

Issue:

In the function createStake in TokenStaking contract there is wrong rewards calculation for the previous staked amount, because users' stakes balance will be increased before rewards calculation, so users also will get rewards for the new staking tokens amount. (TokenStaking.sol)

Recommendation:

We recommend to calculate rewards amount before increasing the users staking balance (stakes mapping).

Fixed:

Issue fixed by the contract creator at 13.10.2020.

2. Wrong condition in function setSupplyCap

Issue:

In function setSupplyCap(uint _supplyCap) at line 175 there is a wrong if statement condition, so the address with role _SUPPLY will not be able to increase total supply amount, just to decrease it, but should be vice versa. Because of this there could appear the situation, that amount of tokens in user accounts will be more, than total cap. (Fundamenta.sol)

Recommendation:

Change the if statement condition.

Fixed:
Issue fixed by the contract creator at 13.10.2020.

Medium Severity Issues

1. **Wrong withdraw rewards calculation**

Issue:
Amount of withdrawn rewards in TokenStaking contract will be calculated wrongly, because there is no increase of users paid rewards amount in functions createStake, removeStake, emergencyWithdrawRewardAndStakes. (TokenStaking.sol)

Recommendation:

Add increasing of paid rewards amount in this functions.

Fixed:
Issue fixed by the contract creator at 13.10.2020.

2. **Wrong Unlock height**

Issue:
In function addPosition there is a wrong unlock height calculation in third if statement at line 437. There should be multiplication by lockPeriod2, but there is lockPeriod0. (LiquidityMining.sol)

Recommendation:

Change lockPeriod0 to lockPeriod2.

Fixed:
Issue fixed by the contract creator at 13.10.2020.

Low Severity Issues

1. **No checking for correctness of new lock periods**

Issue:
In the function setLockPeriods there is no checking that new lock periods will be correct numbers, there could appear the situation, when these numbers will be smaller than now, for example. (LiquidityMining.sol)

Recommendation:

Add checking for correctness of lock periods.

Fixed:
Issue fixed by the contract creator at 13.10.2020.

2. Burning from any address

Issue:
Address with the role burner could burn from any address without checking the allowed amount for burning. (Fundamenta.sol)

Recommendation:
We recommend checking for the allowed amount, before burning from any address.

Conclusion

Smart contracts contain only low severity issues and could be deployed to the mainnet.

Audit performed by Ilnar K. and Matthew L.