PRF Network

Smart Contract Security Audit

December, 2020

TechRate

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 PRF Network to perform an audit of smart contracts:

- ***Network.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.

Token Economy Model

BASIC CONDITIONS.
1. The Network smart contract does not have a beneficiary or other affiliated persons receiving an individual reward over standart Network marketing.
2. You can exchange Ethereum (ETH) for Network tokens (NET) only after receiving a registration transfer from the address previously registered on the Network smart contract.
3. The linking of the subscriber (referral) address is carried out by transferring to it any number of NET, provided that no one has done this yet, and the referral link cannot be changed under any circumstances, except for the situation described in p.4.
4. Important! If at the time of accrual of the referral reward the balance of the address is less than 0.0625 NET, the referrer address of the referral chain lower address will be replaced with the address of a higher referral chain address. In other words, the subordinate address will be moved to upstream address in the referral chain. This action is irreversible and affects only the referral chain and the associated marketing conditions of the Network smart contract.
5. The exchange of NET for ETH is carried out by making an ETH deposit to the Network smart contract address and NET issuing.
6. The minimum exchange amount is 1 GWEI (0.000000001 ETH).
7. The exchange rate of NET for ETH at the time of exchange is calculated by the formula:
   R = E / S
   where
   R - exchange rate NET for ETH;
   E - the total amount of ETH deposit placed on the balance of the Network smart contract;
   S - the total emission of NET.
8. At the time of depositing (exchanging) ETH for the Network smart contract, the current rate is calculated and 70% of the received amount is NET issued to the address from which ETH deposit was placed (transferred), and the remaining amount is distributed according to

the referral chain ten levels up, starting from 15% for the address of the first level and further with a decrease in the amount of issue and accrual of NET by half at each next level.
9. To receive a reward from the referral chain, the address balance must have at least 0.0625 NET to receive rewards from the first lower level with a doubling for each subsequent level in depth to the tenth level. Thus, in order to receive a reward from 10 levels, the address must have at least 32 NET. The amount of the referral reward received depends on the balance of the address at the time of calculation. If the balance of the address is greater than or equal to the total potential amount of NET issue according to the placed ETH deposit, the full amount of remuneration is accrued according to the Network marketing, otherwise the remuneration is calculated using the formula:

R = B / D * E

where

R - received remuneration;

B - address balance;

D - amount of potentially issued NET per placed ETH deposit;

E - total amount of remuneration by level according to Network Marketing.

10. For the missed or reduced reward, NET are not issued, thereby increasing the ratio of the total amount of ETH deposit to the total number of NET.
12. The reverse exchange (return) of the deposit is carried out by transferring NET to the address of the Network smart contract, while ETH deposit will be returned to the address that sent the tokens at the rate according to the formula specified in p.7.
13. NET tokens received at the address of the smart contract are destroyed, thereby providing a positive growth trend in the exchange rate of NET for ETH, except for the situation described in p.14.
14. From the launch of Network smart contract until the total emission of 50 NET is reached, the exchange rate is fixed at 1 NET = 1 ETH by issuing the missed and unreceived reward on the balance of the Network smart contract. When the total token emission of 50 NET is reached, all NET on the balance of the smart contract are destroyed (burned) and a dynamic token exchange rate is established.
15. Any address that is the only address with a positive NET balance can reset it's balance, the balance of Network smart contract, withdraw all deposited ETH on the smart contract by using RESTART function. In this case, the exchange rate will return to 1:1 and will be fixed until the emission of 50 NET is reached.
17. For ease of use, the RATE function of smart contract displays the exchange rate of 1 NET for 1 ETH multiplied by 1'000'000 due to the lack of the ability to display floating point numbers in the Ethereum EVM, is for informational purposes only and is not used in calculating actual values within the smart contract marketing and functionality.
18. NET supports all the generally accepted functions and properties of the ERC20 standard on the Ethereum blockchain, incl. transfers, storage and decentralized applications.

Issues Checking Status

No.	Issue description.	Checking status
1	Compiler warnings.	No issues identified
2	Race conditions and Reentrancy. Cross-function race conditions.	No issues identified
3	Possible delays in data delivery.	No issues identified
4	Oracle calls.	No issues identified
5	Front running.	No issues identified
6	Timestamp dependence.	No issues identified
7	Integer Overflow and Underflow.	No issues identified
8	DoS with Revert.	No issues identified
9	DoS with block gas limit.	No issues identified
10	Methods execution permissions.	No issues identified
11	Economy model. If application logic is based on an incorrect economic model, the application would not function correctly and participants would incur financial losses. This type of issue is most often found in bonus rewards systems, Staking and Farming contracts, Vault and Vesting contracts, etc.	No issues identified
12	The impact of the exchange rate on the logic.	No issues identified
13	Private user data leaks.	No issues identified
14	Investors safety. Analyzing whether the owners/developers/governors of the contract are able to illegally withdraw the funds out of the contract (steal/fraud abilities)	No issues identified

Security Issues

High Severity Issues

Smart contract does not contain high severity issues.

Medium Severity Issues

Smart contract does not contain medium severity issues.

Low Severity Issues and Recommendations

Smart contract does not contain low severity issues.

Conclusion

Some low severity issues found and recommendations added.