Jorge Rodriguez

CYBERSEC CONTRACT AUDIT REPORT
Rise - CTDSEC.com

Introduction

During January of 2021, Rise engaged CTDSec to audit smart contracts that they created. The engagement was technical in nature and focused on identifying security flaws in the design and implementation of the contracts. Rise provided CTDSec with access to their code repository and whitepaper.

Disclaimer

It should be noted that this audit is not an endorsement of the reliability or effectiveness of the contract, rather limited to an assessment of the logic and implementation. In order to ensure a secure contract that's able to withstand the Ethereum network's fast-paced and rapidly changing environment, we at CTDSec recommend that the Rise team put in place a bug bounty program to encourage further and active analysis of the smart contract.

Coverage

Target Code and Revision

For this audit, we performed research, investigation, and review of the Rise contract followed by issue reporting, along with mitigation and remediation instructions outlined in this report. The following code files are considered in-scope for the review:

- Rebaser.sol
- Rise.sol
- RiseSafeMath.sol

Attacks made to the contract

In order to check for the security of the contract, we tested several attacks in order to make sure that the contract is secure and follows best practices.

Correctness of the protocol implementation [Result OK]

User funds are secure on the blockchain and cannot be transferred without user permission [Result OK]

Vulnerabilities within each component as well as secure interaction between the network components [Result OK]

Correctly passing requests to the network core [Result OK]

Data privacy, data leaking, and information integrity [Result OK]

Susceptible to reentrancy attack [Result OK]

Key management implementation: secure private key storage and proper management of encryption and signing keys [Result OK]

Handling large volumes of network traffic [Result OK]

Resistance to DDoS and similar attacks [Result OK]

Aligning incentives with the rest of the network [Result OK]

Any attack that impacts funds, such as draining or manipulating of funds [Result OK]

Mismanagement of funds via transactions [Result OK]

Inappropriate permissions and excess authority [Result OK]

Special token issuance model [Result OK]

Vulnerabilities

ISSUES

It has not been possible to carry out any attack scenario since the contract was secure.

Contract transparency

The owner can't disable trading once made enabled.

```
897     function _enableTrading() external onlyOwner() {
898         tradingEnabled = true;
899         TradingEnabled();
900     }
901 }
```

Mint functions can't be used for irregular purposes.

Architecture

Since the images are too large and cannot be attached to the document due to loss of quality, we attach hyperlinks to be able to view them correctly.

Rise Architecture: https://pasteboard.co/JMmgcTc.png

Summary of the Audit

The contracts are safe and have attractive features.

The contract is correctly applied according to token economics.

After reviewing the contract we came to the conclusion that is safe to deploy.