0x Guard

Smart contracts security assessment

Final report

Tariff: Standard

Ravelin Finance

May 2022

0xguard.com

hello@0xguard.com

Contents

Introduction

This report has been prepared for the Ravelin Finance team upon their request.

The audited project is a fork of the Tomb Finance Project.

The purpose of this audit was to ensure that no issues were introduced with the changes to the original code and that known vulnerabilities (e.g. circumventing the protocol’s fee system) are fixed prior to deployment.

Further details about Ravelin Finance are available at the official website: https://www.ravelin.finance/boardroom.

Name	Ravelin Finance
Audit date	2022-05-16 - 2022-05-16
Language	Solidity
Platform	Milkomeda

Contracts checked

Name	Address
RAV	https://explorer-mainnet-cardano-evm.c1.milkomeda.com/address/0x9B7c74Aa737FE278795fAB2Ad62dEFDbBAedFBCA/contracts
RBond	https://explorer-mainnet-cardano-evm.c1.milkomeda.com/address/0xf1F1E08844E9AC3DadcBba349D6D93F1FCaC651f/contracts
RShare	https://explorer-mainnet-cardano-evm.c1.milkomeda.com/address/0xD81E377E9cd5093CE752366758207Fc61317fC70/contracts

RShareRewardPool	https://explorer-mainnet-cardano-evm.c1.milkomeda.com/address/0xa85B4e44A28B5F10b3d5751A68e03E44B53b7e89/contracts
Treasury	https://explorer-mainnet-cardano-evm.c1.milkomeda.com/address/0x351bDAC12449974e98C9bd2FBa572EdE21C1b7C4/contracts
Oracle	https://explorer-mainnet-cardano-evm.c1.milkomeda.com/address/0x6B089a6bc16F43120F39dC1BdB4825046E33dF16/contracts
Boardroom	https://explorer-mainnet-cardano-evm.c1.milkomeda.com/address/0x618C166262282DcB6Cdc1bFAB3808e2fa4ADFEc2/contracts
Multiple contracts	

Procedure

We perform our audit according to the following procedure:

Automated analysis

- Scanning the project's smart contracts with several publicly available automated Solidity analysis tools
- Manual verification (reject or confirm) all the issues found by the tools

Manual audit

- Comparing the project to the Tomb Finance implementation

Classification of issue severity

High severity

High severity issues can cause a significant or full loss of funds, change of contract ownership, major interference with contract logic. Such issues require immediate attention.

Medium severity	Medium severity issues do not pose an immediate risk, but can be detrimental to the client's reputation if exploited. Medium severity issues may lead to a contract failure and can be fixed by modifying the contract state or redeployment. Such issues require attention.
Low severity	Low severity issues do not cause significant destruction to the contract's functionality. Such issues are recommended to be taken into consideration.

Issues

High severity issues

No issues were found

Medium severity issues

No issues were found

Low severity issues

1. Reentrancy attack (RShareRewardPool)

When withdrawing, some pool tokens may be subject to a reentrancy attack. The variable `user.rewardDebt` in `withdraw()` function is updated after calling `pool.token.safeTransfer()`.

Recommendation: It is recommended to update the value of the `user.rewardDebt` variable before calling `pool.token.safeTransfer()`.

2. Few events (Multiple contracts)

Many set functions from contracts are missing events when changing important values in the contact.

Recommendation: Create events for these set functions.

Conclusion

2 low severity issues were found.

The Ravelin Finance Project was compared with the Tomb Project. Ravelin Finance has changed the implementation of Token contract.

The changed contracts is not affected by the vulnerability that was discovered in the Tomb before because it doesn't contain the implementation of transfer with taxes.

Disclaimer

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability)set forth in the Services Agreement, or the scope of services, and terms and conditions provided to the Company in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes without 0xGuard prior written consent.

This report is not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any “product” or “asset” created by any team or project that contracts 0xGuard to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

0x Guard