Guard

Smart contracts security assessment

Final report

Tariff: Standard

Rare Finance

March 2022

0xguard.com

hello@0xguard.com

Contents

Introduction

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

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

Further details about Rare Finance are available at the official website: https://rarefinance.biz/

Name	Rare Finance
Audit date	2022-03-11 - 2022-03-11
Language	Solidity
Platform	Fantom Network

Contracts checked

Name	Address
RShare	0xB835631824ED68D84c5f41C231f3C2b6C2D709d5
Rare Reward Pool	0x866ca87e17f06b508301dc8523e46330dfdd3086
RBond	0x8ee50DCDDE97895a53206FAC81f1C9Cc10d0A15e
Treasury	0x0CE08F1B7f648DcEe7008b8c7EC5c57C5d149196
Masonry	0xf101c91B35f83509e51f0C34b3BBc358a97A11B1
Rare	0x428F578F88351487f3D9e5F3F39f66976e5588C2
Oracle	0xb6A825b34B24203C31B68A60B5aaE279633Eb9E5

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

No issues were found

Conclusion

The Rare Finance Project was compared with the Tomb Project. Rare Finance has changed the implementation of RareRewardPool and RshareRewardPool contracts.

In the RareRewardPool and RShareRewardPool contracts reward distribution was changed. In the RareRewardPool added logics with daoFund address.

The changed Token contract is not affected by the vulnerability that was discovered in the Tomb Project since the TAX collection functionality is not used in the deployed contract at address 0x428F578F88351487f3D9e5F3F39f66976e5588C2.

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