0x Guard

Smart contracts security assessment

Final report

Tariff: Standard

Arctic Fox Finance

March 2022

0xguard.com

hello@0xguard.com

Contents

Introduction

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

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

Further details about Arctic Fox Finance are available at the official website: https://arctic-fox.finance/

Name	Arctic Fox Finance
Audit date	2022-03-30 - 2022-03-31
Language	Solidity
Platform	Avalanche Network

Contracts checked

Name	Address
FOX	https://snowtrace.io/address/0xFFffFfFf68A2e13F7B68d2E190E37D804E02E0ad#code
FOXSHARE	https://snowtrace.io/address/0x510c4d8ECB31d2f7f258728B65bB388023b2001c#contracts
FOXBOND	https://snowtrace.io/address/0xF0A26def94FC0c37fB358f5dcACd78cE6ac88184#code
Treasury	https://snowtrace.io/address/0x903f91e89e78F0c6D00dE69b420253C1554b0743#code
RebateTreasury	https://snowtrace.io/address/0x039754D5Cb54370De974eA21D6325B80eb97a13A#code
Masonry	https://snowtrace.io/address/0x6d9F71132C421f29Ff4c85b87b9dfDaF1dfFe7eB#code
GenesisPool	https://snowtrace.io/address/0xa0CF3b97E60DC5C83b4f4d598F290F89eF411851#code

SharePool	https://snowtrace.io/address/0x2DD976A40c4f052FaD33ECf7C16a18B535b44316#code
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

1. Tax bypass (FOX)

Tax avoidance in the Tomb project is the main problem the team faced. The problem is that there is an invariant in the `transferFrom()` function that deducts tax for the transfer of tokens, but there is also an invariant without deduction of tax that calls the `transfer()` function. With the help of this problem, you can bypass all tax deductions if you use only the `transfer()` function and it is possible to violate the tokenomics of the project.

Recommendation: It is recommended to overload the `transfer()` function to work with tax or completely remove the tax functionality in contracts.

Medium severity issues

1. Contract ownership (Multiple contracts)

1) The projects owner can change the `taxRate` in FOX token up to 100% in the `setTaxRate()` function if you change the `taxOffice` in the `setTaxOffice()` function to a compromised address.

2) Operator can change `taxTiersTwaps` and `taxTiersRate` up to 100% in FOX token in `setTaxTiersTwap()` and `setTaxTiersRate()` functions.

3) The Operator role can change the addresses of funds in the Treasury contract using the function `setExtraFunds()` function. The `daoFund` can be withdrawn if the operator account is compromised.

Recommendation: There are a large number of functions with the `onlyOperator()` modifier, there is a possibility that the operator can be compromised. It is recommended to create multiple roles for different kinds of functions to reduce the operator's problem. It is also recommended to add a time

delay to the especially important set functions using the TimelockController. We also recommend that you look through the entire codebase to find functions that are dangerous for you as the owner of the project (mainly set functions), if there are any, then add a call to them via multisig wallet. This will help avoid the issue of owner compromise.

Low severity issues

1. Unused variable (GenesisPool)

State variable `shiba` is not used anywhere.

Recommendation: Remove all references to this variable from the contract.

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

Arctic Fox Finance FOX, FOXSHARE, FOXBOND, Treasury, RebateTreasury, Masonry, GenesisPool, SharePool, Multiple contracts contracts were audited. 1 high, 1 medium, 2 low severity issues were found.

The Arctic Fox Finance Project was compared with the Tomb Project. Arctic Fox Finance has changed the implementation of `GenesisPool` and `Treasury` contracts. Added a new contract - `RebateTreasury`.

Added automatic sending of a certain percentage of FoxBond to `RebateTreasury` in the `Treasury` contract.

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