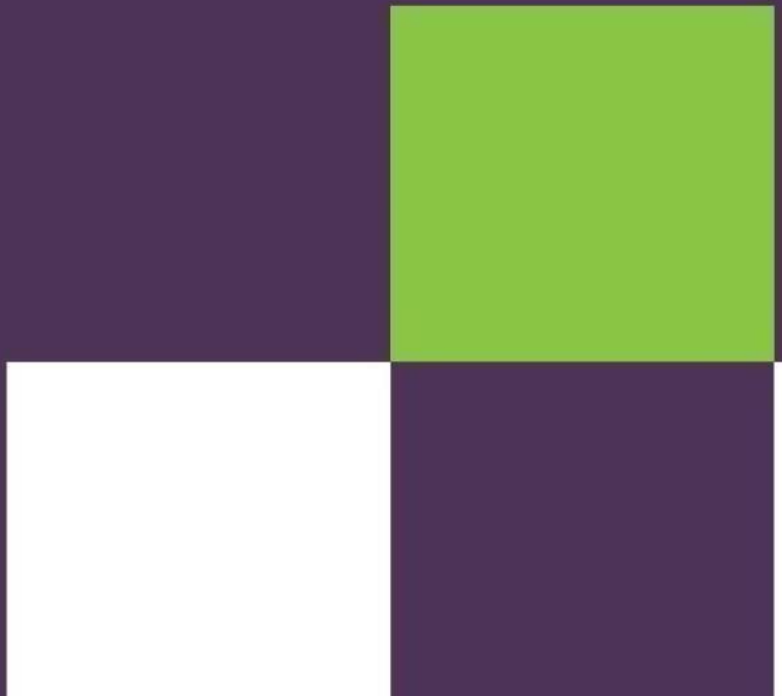
Audit Whale

Smart contract code review and security analysis report



This document may contain confidential information about IT systems and the intellectual property of the Customer as well as information about potential vulnerabilities and methods of their exploitation.

The report containing confidential information can be used internally by the Customer, or it can be disclosed publicly after all vulnerabilities are fixed — upon a decision of the Customer.

Document

Name	Smart Contract Code Review and Security Analysis Report for FantomYields.
Approved by	Jameson | COO AuditWhale
Type	---
Platform	All Chains
Methods	Architecture Review, Functional Testing, Computer-Aided Verification, Manual Review
Repository	---
Commit	---
Technical Documentation	NO
JS tests	NO
Website	fantomyields.com
Timeline	26 FEB 2022– 28 FEB 2022
Change log	28 FEB 2022 – INITIAL AUDIT

Table of contents

Introduction

AuditWhale(Consultant) was contracted by FantomYields (Customer) to conduct a Smart Contract Code Review and Security Analysis. This report presents the findings of the security assessment of the Customer's smart contract and its code review conducted between 26 FEB 2022– 28 FEB 2022.

Scope

The scope of the project is smart contracts in the repository:
Here are some of the commonly known vulnerabilities that are considered:

Category	Check Item
Code review	▪ Reentrancy ▪ Ownership Takeover ▪ Timestamp Dependence ▪ Gas Limit and Loops ▪ DoS with (Unexpected) Throw ▪ DoS with Block Gas Limit ▪ Transaction-Ordering Dependence ▪ Style guide violation ▪ Costly Loop ▪ Unchecked external call ▪ Unchecked math ▪ Unsafe type inference ▪ Implicit visibility level ▪ Deployment Consistency ▪ Repository Consistency ▪ Data Consistency

Functional review	▪ Business Logics Review ▪ Functionality Checks ▪ Access Control & Authorization ▪ Escrow manipulation ▪ Token Supply manipulation ▪ Assets integrity ▪ User Balances manipulation ▪ Data Consistency manipulation ▪ Kill-Switch Mechanism ▪ Operation Trails & EventGeneration

Executive Summary

According to the assessment, the Customer's smart contracts are well-secured.

Our team performed an analysis of code functionality, manual audit, and automated checks with Jameson. All issues found during automated analysis were manually reviewed, and important vulnerabilities are presented in the Audit overview section. All found issues can be found in the Audit overview section.

As a result of the audit, security engineers found 1 low severity issue.

Project	Contract Address	Project Address	Network
Fantom	https://ftmscan.com/address/0x8f87e9858c22c3ac63526d1b0c1bbb37a7faa870	0x8f87e9858c22c3ac63526d1b0c1bbb37a7faa870	ftmscan

Referral System (Match Bonus):

- Level -1 5%
- Level -2 4%
- Level -3 3%

Notes:

- Referral should be an active user; it means the referral address has at least one deposit
- If the user has not had a valid upline, the owner will be set as default upline.

Audit overview & Severity Definitions:

CRITICAL ISSUES (critical,high severity):	0
HIGH ISSUES (high, medium severity):	2
ERRORS, WARNINGS (medium, low severity):	0
OPTIMIZATION (low severity):	1
RECOMMENDATIONS (very low severity):	0

High ISSUE:

- The system used is called ROI and must be considered as HIGH-RISK.
- Users can withdraw only once a day
- Users principal deposits cannot be withdrawn, users can get dividends and referral commission. Dividends are paid from deposits of other users. Do always invest with proper knowledge and investigation

Optimization suggestions:

Loop on the dynamic variable (low severity).

If the user gets more parallel deposits his withdrawal transaction going to cost more transaction fee because the loop on the dynamic variable is used in the 'withdraw' function.

Caution:
In case exceeding the GAS limit of the size of the transaction game play is not possible.

Independent description of the smart-contract functionality:

The FantomYields smart contract provides the opportunity to invest any amount in Fantom (10$ worth) in the contract and get up to 300% return on investment in 10 days if the contract balance has enough funds for payment..

Conclusion

In the FantomYields Smart-Contract were found no vulnerabilities, no backdoors, and no scam scripts.

The code was tested with compatible compilers and simulated manually reviewed for all commonly known and specific vulnerabilities.

So FantomYields Smart-Contract is safe for use in the All Chain main networks.

Disclaimers

This audit is only to the Smart-Contract code at the specified address.

Audit Whale is a 3rd party auditing company that works on audits based on client requests. And as a professional auditing firm, we check on the contract for any vulnerabilities, backdoors, and/or scam scripts.

Therefore:

We are not financial advisors nor do we partner with the contract owners

Operations and website administration is fully on the client's side

We do not have influence over client operations, which can lead to website changes, withdrawal function closes, etc. One always has the option to do this through the contract.

Any concerns about the project themselves need to be raised directly to the project owners and not through Audit Whale.

Investors are not in any way obliged, coerced or influenced to invest in projects audited by Audit Whale.

We are not responsible for your funds or guarantee you profits.

We highly recommend that investors do their own research and gain crypto experience before investing