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 CandyDex.
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	Candydex.finance
Timeline	19 Apr 2022– 23 Apr 2022
Change log	23 Apr 2022 – INITIAL AUDIT

Table of contents

Introduction

AuditWhale(Consultant) was contracted by CandyDex (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 19 Apr 2022– 23 Apr 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
CANDYDEX	https://polygonscan.com/address/0xabe1a652cbc6eb1782b5de4e800f8bf714aaf5d0	0xabe1a652cbc6eb1782b5de4e800f8bf714aaf5d0	MATIC

Audit overview & Severity Definitions:

CRITICAL ISSUES (critical,high severity):	**0**
HIGH ISSUES (high, medium severity):	**6**
ERRORS, WARNINGS (medium, low severity):	**0**
OPTIMIZATION (low severity):	**1**
RECOMMENDATIONS (very low severity):	**0**

High ISSUE:

- **The Contract is enabled with the option to restrict transfer till IDO completes,**
- **Ownership can be transferred in this system.**
- **Admin can change the IDO end date any time and can restrict the transfer for normal transfer.**
- **Admin has the option to blacklist the user account and the blacklisted accounts can only send back the tokens to the contract owner address, this is specific care taker for token if tokens get to wrong hands**
- **MATIC cannot be sent to the contract address and a revert was initiated if user transfer funds to this account**
- **Admin can transfer tokens if there are any tokens transferred to this contract address,**

Optimization suggestions:

Transaction failure till IDO complete.

If the user gets error the errors are clear and the reason is displayed in the contract address with clear explanations on the reason of failure. no specific necessity of increased gas limit for transaction approval while user initiates a transfer.

Caution:

In case of failed transaction, please check the reason, the reason is quite open here with the contract.

Independent description of the smart-contract functionality:

The CandyDex smart contract provides the opportunity to invest any amount in CANDYDEX (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 CandyDex 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 CandyDex 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